Ruby - Feature #6946

FIPS support?

08/28/2012 09:31 PM - vo.x (Vit Ondruch)

Status:	Open
Priority:	Normal
Assignee:	
Target version:	

Description

=begin
Hi, running the test suite on FIPS enabled system using

$ find test/ -type f -name test_*.rb -exec make test-all TESTS="-v '{}'" ;

command with patch from #6938 applied, it gives me a plenty of errors (see attached output.txt file). There are two kind of errors as far as I understand, some are more or less test suite errors (e.g. #6938), which should be easy to fix, while some others (e.g. #6943) would need bigger changes.

Is there any chance that Ruby will provide better support for FIPS and there errors get fixed?
=end

Related issues:

Related to Ruby - Bug #6938: [PATCH] Increase DH key size to fix test suite i...	**Closed**	**08/28/2012**
Related to Ruby - Feature #6943: pstore in FIPS mode	**Closed**	

Associated revisions

Revision e29819df - 09/03/2012 01:14 AM - MartinBosslet (Martin Bosslet)

- ext/openssl/extconf.rb: Detect OpenSSL_FIPS macro
  ext/openssl/ossl.c: Expose OpenSSL::OPENSSL_FIPS constant to
  indicate whether OpenSSL runs in FIPS mode.
  test/openssl/test_pkey_dh.rb: Generate 256 bit keys for
  non-FIPS installations to improve test performance (e.g. for
  rubyci).
  test/openssl/utils.rb: Replace DSS1 as certificate signature
  digest with SHA1 for FIPS installations when using DSA by
  introducing TestUtils::DSA_SIGNATURE_DIGEST.
  test/openssl/test_x509cert.rb:
  test/openssl/test_x509crl.rb:
  test/openssl/test_x509req.rb: Use DSA_SIGNATURE_DIGEST
  NEWS: Introduce OpenSSL::OPENSSL_FIPS

  These changes allow running the OpenSSL tests in FIPS mode
  while keeping a high performance for non-FIPS installations.
  Introduction of OpenSSL::OPENSSL_FIPS allows for applications
  to react to special requirements when using OpenSSL in FIPS mode.
  [Feature #6946] [ruby-core:47345]

- Diese und die folgenden Zeilen werden ignoriert --

M ext/openssl/extconf.rb
M ext/openssl/ossl.c
M NEWS
M ChangeLog
M test/openssl/utils.rb
M test/openssl/test_x509crl.rb
M test/openssl/test_x509req.rb
M test/openssl/test_x509cert.rb
M test/openssl/test_pkey_dh.rb

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36884 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision b6c38f67 - 09/03/2012 10:13 PM - MartinBosslet (Martin Bosslet)

- Reference feature #6946 in Changelog entry.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36893 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a3b753b2 - 12/20/2012 12:29 AM - MartinBosslet (Martin Bosslet)

- ext/openssl/ossl.c: add OpenSSL.fips_mode= to allow enabling FIPS mode manually.
- test/openssl/utils.rb: turn off FIPS mode for tests. This prevents OpenSSL installations with FIPS mode enabled by default from raising FIPS-related errors during the tests.
- test/openssl/test_fips.rb: add tests for FIPS-capable OpenSSL installations.
  [Feature #6946] [ruby-core:47345]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@38480 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 4fce754f - 12/20/2012 07:00 AM - MartinBosslet (Martin Bosslet)

- ext/openssl/ossl.c: do not use FIPS_mode_set if not available.
- test/openssl/utils.rb: revise comment about setting FIPS mode to false.
- test/openssl/test_fips.rb: remove tests that cause errors on ruby-ci.
  [Feature #6946] [ruby-core:47345]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@38491 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 08/28/2012 09:36 PM - MartinBosslet (Martin Bosslet)

- Category set to ext

- Assignee set to MartinBosslet (Martin Bosslet)

- Target version set to 2.0.0

Sure, I'll look into it while applying your patch from #6938!

#2 - 08/29/2012 04:20 AM - MartinBosslet (Martin Bosslet)

- Status changed from Open to Assigned

#3 - 09/02/2012 10:01 PM - MartinBosslet (Martin Bosslet)

I believe the proper way to handle differences in FIPS mode is to expose a handle that allows to detect whether we are running in FIPS mode or not. That way we can configure appropriate algorithms and key sizes in the tests. This should make it possible to run tests quickly when not using FIPS (as needed by rubyci) while still offering better support for running the tests in FIPS mode. Working on that now.

#4 - 09/02/2012 10:29 PM - vo.x (Vit Ondruch)

Sounds reasonable. Thank you!

#5 - 09/03/2012 10:14 AM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r36884.
Vit, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/openssl/extconf.rb: Detect OpenSSL_FIPS macro
  ext/openssl/ossl.c: Expose OpenSSL::OPENSSL_FIPS constant to indicate whether OpenSSL runs in FIPS mode.

test/openssl/test_pkey_dh.rb: Generate 256 bit keys for
non-FIPS installations to improve test performance (e.g. for
rubyci).
test/openssl/utils.rb: Replace DSS1 as certificate signature
digest with SHA1 for FIPS installations when using DSA by
introducing TestUtils::DSA_SIGNATURE_DIGEST.
test/openssl/test_x509cert.rb:
test/openssl/test_x509crl.rb:
test/openssl/test_x509req.rb: Use DSA_SIGNATURE_DIGEST
NEWS: Introduce OpenSSL::OPENSSL_FIPS

These changes allow running the OpenSSL tests in FIPS mode
while keeping a high performance for non-FIPS installations.
Introduction of OpenSSL::OPENSSL_FIPS allows for applications
to react to special requirements when using OpenSSL in FIPS mode.
[Feature #6946] [ruby-core:47345]

- Diese und die folgenden Zeilen werden ignoriert --

M ext/openssl/extconf.rb
M ext/openssl/ossl.c
M NEWS
M ChangeLog
M test/openssl/utils.rb
M test/openssl/test_x509crl.rb
M test/openssl/test_x509req.rb
M test/openssl/test_x509cert.rb
M test/openssl/test_pkey_dh.rb

#6 - 09/03/2012 10:53 AM - MartinBosslet (Martin Bosslet)

The applied changes now allow us to tweak algorithms/key lengths with respect to running in FIPS mode or not.

@Vit: Could you please confirm that this improves the situation with regard to OpenSSL tests? Could you provide me a list of the tests that still fail on your side? I'm using OpenSSL 1.0.1c and openssl-fips-2.0.1 on my side, but it let for example MD5 tests pass while it's not supposed to...

#7 - 09/03/2012 01:06 PM - naruse (Yui NARUSE)

- Status changed from Closed to Assigned

r36884 breaks CentOS 5.6 with OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008
http://c5632.rubyci.org/~chkbuild/ruby-trunk/log/20120903T030102Z.log.html.gz
http://c5664.rubyci.org/~chkbuild/ruby-trunk/log/20120903T030301Z.log.html.gz

#8 - 09/04/2012 07:13 AM - Anonymous

- Status changed from Assigned to Closed

This issue was solved with changeset r36893.
Vit, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- Reference feature #6946 in Changelog entry.

#9 - 09/04/2012 07:23 AM - MartinBosslet (Martin Bosslet)

What a mess. Versions prior to 1.0.0 (FIPS, too) require DSS1 as the digest to be used in conjunction with DSA. DSS1 is just SHA-1 under a different name. Now while non-FIPS >= 1.0.0 allows both DSS1 and SHA-1, the FIPS version suddenly forbids DSS1 and now requires SHA-1... o_O

#10 - 09/04/2012 04:29 PM - vo.x (Vit Ondruch)

- File output-r36887.txt added

- Status changed from Closed to Open

It is getting better, but there is still a lot of failing tests. Please see attached output-r36887.txt. Thank you.

#11 - 09/04/2012 10:27 PM - MartinBosslet (Martin Bosslet)

vo.x (Vit Ondruch) wrote:

> It is getting better, but there is still a lot of failing tests. Please see attached output-r36887.txt. Thank you.

Thank you for the list! Something is totally wrong with the FIPS module I compiled. It happily accepts MD5. May I ask what combination (FIPS and regular OpenSSL) you used to get those results?

#12 - 09/05/2012 03:53 PM - vo.x (Vit Ondruch)

This is my OpenSSL version:

rpm -q openssl-libs

openssl-libs-1.0.1c-1.el7.x86_64

However, I am unsure, what other information you need. There is no FIPS Kernel module to my knowledge (but my knowledge is limited :/).

#13 - 09/07/2012 12:07 AM - MartinBosslet (Martin Bosslet)

- Status changed from Open to Assigned

vo.x (Vit Ondruch) wrote:

> This is my OpenSSL version:
>
> # rpm -q openssl-libs
>
> openssl-libs-1.0.1c-1.el7.x86_64
>
> However, I am unsure, what other information you need. There is no FIPS Kernel module to my knowledge (but my knowledge is limited :/).

OK, I see. So at least you are using the same basic OpenSSL library version as I am. I need to investigate if something went wrong while building my FIPS module. Thanks!

#14 - 10/25/2012 04:31 PM - ko1 (Koichi Sasada)

ping. status?

#15 - 11/24/2012 09:24 AM - mame (Yusuke Endoh)

Martin Bosslet, what's the status?

--
Yusuke Endoh mame@tsg.ne.jp

#16 - 11/24/2012 01:31 PM - mame (Yusuke Endoh)

- Target version changed from 2.0.0 to 2.6

#17 - 12/19/2012 01:16 PM - MartinBosslet (Martin Bosslet)

I'm sorry for not responding earlier. The problem is that I simply can't get a FIPS version of OpenSSL linked with Ruby OpenSSL to complete this task. I'm trying OpenSSL 1.0.1c and openssl-fips-2.0.2. I can compile my 1.0.1c using the FIPS canister, and I also verified that FIPS mode is working correctly.

The problem is now linking the Ruby OpenSSL extension against it. I'm supposed to include /usr/local/ssl/fips-2.0/bin/ in $PATH and then to compile using

```
make CC=fipsld FIPSLD_CC=gcc
```

On my 32 bit Linux machine this gives me a segfault during the linking phase and on my 64 bit machine I get:

linking shared-object openssl.so
/usr/bin/ld: /tmp/cc1Oph68.o: relocation R_X86_64_32S against `.rodata' can not be used when making a shared object; recompile with -fPIC
/tmp/cc1Oph68.o: could not read symbols: Bad value
collect2: ld returned 1 exit status
make: *** [openssl.so] Error 1

I checked, both the FIPS canister as well as OpenSSL were compiled using -fPIC, and -fPIC is also part of the CFLAGS in the Makefile generated for the OpenSSL extension. Ruby itself was compiled using -fPIC, too. The OpenSSL C library was linked statically (libcrypto.a & libssl.a). gcc version is

gcc version 4.6.3 (Ubuntu/Linaro 4.6.3-1ubuntu5)

I'd appreciate any help, I'm really stuck here. Has anyone got an idea what I do wrong or has anyone had success in linking Ruby OpenSSL to a FIPS version of native OpenSSL?

#18 - 12/20/2012 09:29 AM - Anonymous

- Status changed from Assigned to Closed

This issue was solved with changeset r38480.
Vit, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/openssl/ossl.c: add OpenSSL.fips_mode= to allow enabling FIPS mode manually.
- test/openssl/utils.rb: turn off FIPS mode for tests. This prevents OpenSSL installations with FIPS mode enabled by default from raising FIPS-related errors during the tests.
- test/openssl/test_fips.rb: add tests for FIPS-capable OpenSSL installations.
  [Feature #6946] [ruby-core:47345]

#19 - 12/20/2012 09:37 AM - MartinBosslet (Martin Bosslet)

OK, finally got it working. I added OpenSSL.fips_mode= to enable/disable FIPS mode manually. The test suite now automatically disables FIPS mode when running the tests. This worked for my FIPS-enabled version of OpenSSL. I have also added a few tests that specifically assert some things that would be expected to fail in FIPS mode (test_fips.rb).

@Vit: Could you please confirm that this works for you, too?

@mame (Yusuke Endoh): Sorry that I committed this to 2.0.0 even if you already assigned it for next minor. But I felt the approach to adding FIPS support so far was flawed (my mistake) and I wouldn't want a half-assed implementation see to make its way into 2.0.0 - I hope this is OK?

#20 - 12/20/2012 01:53 PM - ko1 (Koichi Sasada)

Some CI servers fail with this modification.
http://rubyci.org/

and also on my development environment (Debian Squeeze) :)

$ make test-all
./ruby: symbol lookup error:
/mnt/sdb1/ruby/build/.ext/x86_64-linux/openssl.so: undefined symbol:
FIPS_mode_set

Could you check it?

FYI:

> $ LANG=C aptitude show openssl
> Package: openssl
> State: installed
> Automatically installed: no
> Version: 0.9.8o-4squeeze13
> Priority: optional
> Section: utils
> Maintainer: Debian OpenSSL Team pkg-openssl-devel@lists.alioth.debian.org
> Uncompressed Size: 2355 k
> Depends: libc6 (>= 2.7), libssl0.9.8 (>= 0.9.8m-1), zlib1g (>= 1:1.1.4)
> Suggests: ca-certificates
> Conflicts: ssleay (< 0.9.2b)
> Description: Secure Socket Layer (SSL) binary and related cryptographic tools
> This package contains the openssl binary and related tools.
>
> It is part of the OpenSSL implementation of SSL.
>
> You need it to perform certain cryptographic actions like:
>
> - Creation of RSA, DH and DSA key parameters;
> - Creation of X.509 certificates, CSRs and CRLs;
> - Calculation of message digests;
> - Encryption and decryption with ciphers;
> - SSL/TLS client and server tests;
> - Handling of S/MIME signed or encrypted mail.

(2012/12/20 9:37), MartinBosslet (Martin Bosslet) wrote:

> Issue #6946 has been updated by MartinBosslet (Martin Bosslet).
>
> OK, finally got it working. I added OpenSSL.fips_mode= to enable/disable FIPS mode manually. The test suite now automatically disables FIPS mode when running the tests. This worked for my FIPS-enabled version of OpenSSL. I have also added a few tests that specifically assert some things that would be expected to fail in FIPS mode (test_fips.rb).
>
> @Vit: Could you please confirm that this works for you, too?
>
> ## @mame (Yusuke Endoh): Sorry that I committed this to 2.0.0 even if you already assigned it for next minor. But I felt the approach to adding FIPS support so far was flawed (my mistake) and I wouldn't want a half-assed implementation see to make its way into 2.0.0 - I hope this is OK?
>
> Feature #6946: FIPS support?
> https://bugs.ruby-lang.org/issues/6946#change-34880
>
> Author: vo.x (Vit Ondruch)
> Status: Closed
> Priority: Normal
> Assignee: MartinBosslet (Martin Bosslet)
> Category: ext
> Target version: next minor
>
> =begin
> Hi, running the test suite on FIPS enabled system using
>
> $ find test/ -type f -name test_*.rb -exec make test-all TESTS="-v '{}'" ;
>
> command with patch from #6938 applied, it gives me a plenty of errors (see attached output.txt file). There are two kind of errors as far as I understand, some are more or less test suite errors (e.g. #6938), which should be easy to fix, while some others (e.g. #6943) would need bigger changes.
>
> Is there any chance that Ruby will provide better support for FIPS and there errors get fixed?
> =end

--
// SASADA Koichi at atdot dot net

#21 - 12/20/2012 04:03 PM - MartinBosslet (Martin Bosslet)

@ko1 (Koichi Sasada): It should work with OpenSSL versions that have no "FIPS_mode_set" now, too. I removed the FIPS-related tests that caused errors on ruby-ci as well!

#22 - 12/20/2012 04:23 PM - ko1 (Koichi Sasada)

After that, I got the following error.

```
make[2]: Entering directory `/mnt/sdb1/ruby/build/ext/openssl'
compiling ../../../trunk/ext/openssl/ossl_x509attr.c
compiling ../../../trunk/ext/openssl/ossl.c
compiling ../../../trunk/ext/openssl/ossl_pkey_dh.c
compiling ../../../trunk/ext/openssl/ossl_x509req.c
compiling ../../../trunk/ext/openssl/ossl_cipher.c
../../../trunk/ext/openssl/ossl_cipher.c: In function 'ossl_get_gcm_auth_tag':
../../../trunk/ext/openssl/ossl_cipher.c:536: error: 'EVP_CTRL_GCM_GET_TAG' undeclared (first use in this function)
../../../trunk/ext/openssl/ossl_cipher.c:536: error: (Each undeclared identifier is reported only once
../../../trunk/ext/openssl/ossl_cipher.c:536: error: for each function it appears in.)
../../../trunk/ext/openssl/ossl_cipher.c: In function 'ossl_cipher_get_auth_tag':
../../../trunk/ext/openssl/ossl_cipher.c:574: error: 'NID_aes_128_gcm' undeclared (first use in this function)
../../../trunk/ext/openssl/ossl_cipher.c:574: error: 'NID_aes_192_gcm' undeclared (first use in this function)
../../../trunk/ext/openssl/ossl_cipher.c:574: error: 'NID_aes_256_gcm' undeclared (first use in this function)
../../../trunk/ext/openssl/ossl_cipher.c: In function 'ossl_set_gcm_auth_tag':
../../../trunk/ext/openssl/ossl_cipher.c:585: error: 'EVP_CTRL_GCM_SET_TAG' undeclared (first use in this function)
../../../trunk/ext/openssl/ossl_cipher.c: In function 'ossl_cipher_set_auth_tag':
../../../trunk/ext/openssl/ossl_cipher.c:616: error: 'NID_aes_128_gcm' undeclared (first use in this function)
../../../trunk/ext/openssl/ossl_cipher.c:616: error: 'NID_aes_192_gcm' undeclared (first use in this function)
../../../trunk/ext/openssl/ossl_cipher.c:616: error: 'NID_aes_256_gcm' undeclared (first use in this function)
../../../trunk/ext/openssl/ossl_cipher.c: In function 'ossl_cipher_is_authenticated':
../../../trunk/ext/openssl/ossl_cipher.c:641: error: 'NID_aes_128_gcm' undeclared (first use in this function)
```

> ../../../trunk/ext/openssl/ossl_cipher.c:641: error: 'NID_aes_192_gcm' undeclared (first use in this function)
> ../../../trunk/ext/openssl/ossl_cipher.c:641: error: 'NID_aes_256_gcm' undeclared (first use in this function)
> make[2]: *** [ossl_cipher.o] Error 1

Do you need other information?

(2012/12/20 16:03), MartinBosslet (Martin Bosslet) wrote:

> Issue #6946 has been updated by MartinBosslet (Martin Bosslet).
>
> ## @ko1 (Koichi Sasada): It should work with OpenSSL versions that have no "FIPS_mode_set" now, too. I removed the FIPS-related tests that caused errors on ruby-ci as well!
>
> Feature #6946: FIPS support?
> https://bugs.ruby-lang.org/issues/6946#change-34888
>
> Author: vo.x (Vit Ondruch)
> Status: Closed
> Priority: Normal
> Assignee: MartinBosslet (Martin Bosslet)
> Category: ext
> Target version: next minor
>
> =begin
> Hi, running the test suite on FIPS enabled system using
>
> $ find test/ -type f -name test_*.rb -exec make test-all TESTS="-v '{}'" ;
>
> command with patch from #6938 applied, it gives me a plenty of errors (see attached output.txt file). There are two kind of errors as far as I understand, some are more or less test suite errors (e.g. #6938), which should be easy to fix, while some others (e.g. #6943) would need bigger changes.
>
> Is there any chance that Ruby will provide better support for FIPS and there errors get fixed?
> =end

--
// SASADA Koichi at atdot dot net

#23 - 12/20/2012 04:53 PM - ko1 (Koichi Sasada)

(2012/12/20 16:14), SASADA Koichi wrote:

> After that, I got the following error.

This issue was introduced at r38488 ?

--
// SASADA Koichi at atdot dot net

#24 - 12/20/2012 04:53 PM - MartinBosslet (Martin Bosslet)

2012/12/20 SASADA Koichi ko1@atdot.net

> After that, I got the following error.
>
> ...
>
> > make[2]: *** [ossl_cipher.o] Error 1
>
> Do you need other information?

No, I forgot to #ifdef... sorry! Fixing...

-Martin

#25 - 12/20/2012 04:53 PM - usa (Usaku NAKAMURA)

Hello,

In message "[ruby-core:51006] Re: [ruby-trunk - Feature #6946] FIPS support?"
on Dec.20,2012 16:32:23, martin.bosslet@gmail.com wrote:

> No, I forgot to #ifdef... sorry! Fixing...

here is a patch.

Index: ext/openssl/ossl_cipher.c

--- ext/openssl/ossl_cipher.c (revision 38491)
+++ ext/openssl/ossl_cipher.c (working copy)
@@ -482,6 +482,7 @@ ossl_cipher_set_iv(VALUE self, VALUE iv)
return iv;
}

+#ifdef EVP_CTRL_GCM_GET_TAG
/*

- call-seq:

- [redacted]

@@ -644,6 +645,12 @@ ossl_cipher_is_authenticated(VALUE self)
return Qfalse;
}
}
+#else /* EVP_CTRL_GCM_GET_TAG /
+# define ossl_cipher_set_auth_data rb_f_notimplement
+# define ossl_cipher_set_auth_tag rb_f_notimplement
+# define ossl_cipher_get_auth_tag rb_f_notimplement
+# define ossl_cipher_is_authenticated rb_f_notimplement
+#endif / EVP_CTRL_GCM_GET_TAG */

/*

- call-seq:

Regards,
--
U.Nakamura usa@garbagecollect.jp

#26 - 12/20/2012 04:53 PM - MartinBosslet (Martin Bosslet)

Thanks, I fixed it already - I used roughly the same approach as usa :)

2012/12/20 U.Nakamura usa@garbagecollect.jp

> Hello,
>
> In message "[ruby-core:51006] Re: [ruby-trunk - Feature #6946] FIPS support?"
> on Dec.20,2012 16:32:23, martin.bosslet@gmail.com wrote:
>
> > No, I forgot to #ifdef... sorry! Fixing...
>
> here is a patch.
>
> # Index: ext/openssl/ossl_cipher.c
>
> --- ext/openssl/ossl_cipher.c (revision 38491)
> +++ ext/openssl/ossl_cipher.c (working copy)
> @@ -482,6 +482,7 @@ ossl_cipher_set_iv(VALUE self, VALUE iv)
> return iv;
> }
>
> +#ifdef EVP_CTRL_GCM_GET_TAG
> /*

- call-seq:

- [redacted]

@@ -644,6 +645,12 @@ ossl_cipher_is_authenticated(VALUE self)
return Qfalse;
}
}
+#else /* EVP_CTRL_GCM_GET_TAG /
+# define ossl_cipher_set_auth_data rb_f_notimplement
+# define ossl_cipher_set_auth_tag rb_f_notimplement
+# define ossl_cipher_get_auth_tag rb_f_notimplement
+# define ossl_cipher_is_authenticated rb_f_notimplement
+#endif / EVP_CTRL_GCM_GET_TAG */

/*

- call-seq:

Regards,

U.Nakamura usa@garbagecollect.jp

#27 - 12/20/2012 08:53 PM - ko1 (Koichi Sasada)

(2012/12/20 16:45), Martin Boßlet wrote:

> Thanks, I fixed it already - I used roughly the same approach as usa :)

Thank you! Now, it works!

--
// SASADA Koichi at atdot dot net

#28 - 12/20/2012 09:10 PM - vo.x (Vit Ondruch)

MartinBosslet (Martin Bosslet) wrote:

> @Vit: Could you please confirm that this works for you, too?

Marting, thank you for your effort. I'll look into it ASAP. Unfortunately I am not sure if I will be able to check it before the end of the year, but I'll try to do my best.

#29 - 12/21/2012 12:27 AM - MartinBosslet (Martin Bosslet)

vo.x (Vit Ondruch) wrote:

> Marting, thank you for your effort. I'll look into it ASAP. Unfortunately I am not sure if I will be able to check it before the end of the year, but I'll try to do my best.

You're welcome! And - no problem. It would be nice if you can confirm that disabling FIPS mode manually does the trick, but no hurry! Happy Holidays!

#30 - 12/21/2012 12:30 AM - MartinBosslet (Martin Bosslet)

@ko1 (Koichi Sasada), @usa (Usaku NAKAMURA): Sorry guys, for breaking the build! But rubyci seems to be free of OpenSSL-related pain again ;)

#31 - 12/22/2012 01:44 AM - vo.x (Vit Ondruch)

- File output-r38509.txt added

- Status changed from Closed to Assigned

MartinBosslet (Martin Bosslet) wrote:

> @Vit: Could you please confirm that this works for you, too?

Martin, there are good news and bad news. The good news is that there is no core dump anymore! That is definitely major improvement. However, there is still plenty of test suite errors, some of them newly introduced. Do you think it is possible to eliminate them?

There is plenty plenty of "Failed to generate key: key size too small" and "key too short" errors for example, which should be pretty easy to solve IMO.

Anyway, I appreciate your effort.

#32 - 01/30/2014 12:33 PM - vo.x (Vit Ondruch)

- File output-200p353.txt added

I am back with FIPS tests. I am testing "ruby 2.0.0p353 (2013-11-22) [x86_64-linux]" on RHEL7 and there are still some issue. However the overall state is now much better then my initial report. Thank you, especially Martin, for the effort.

I'll try to test Ruby 2.1 as well, when I get chance.

#33 - 01/30/2014 03:12 PM - vo.x (Vit Ondruch)

- File output-210p0.txt added

Seems that Ruby 2.1.0 has some regression. Especially RubyGems throws for each test case "/lib/rubygems/test_case.rb:1329:in `initialize': Neither PUB key nor PRIV key: nested asn1 error (OpenSSL::PKey::RSAError)" error.

#34 - 09/13/2015 03:15 AM - zzak (zzak _)

- Assignee changed from MartinBosslet (Martin Bosslet) to 7150

#35 - 06/20/2016 03:05 PM - pvalena (Pavel Valena)

- File output-230p0.txt added

I have attached some more FIPS tests. These can be summarized in comparison with 210p0:

Resolved in 230p0

TestResolvAddr#test_invalid_byte_comment:
NameError: uninitialized constant TestResolvAddr::Tempfile

OpenSSL::TestEngine#test_openssl_engine_cipher_rc4:
OpenSSL::Engine::EngineError: no such cipher `RC4'

OpenSSL::TestDigest#test_digest_constants:
RuntimeError: Unsupported digest algorithm (MD4).

OpenSSL::TestPKCS12#test_create:
OpenSSL::PKCS12::PKCS12Error: encrypt error

OpenSSL::TestPKCS12#test_create_no_pass:
OpenSSL::PKCS12::PKCS12Error: encrypt error

OpenSSL::TestPKCS12#test_create_with_chain:
OpenSSL::PKCS12::PKCS12Error: encrypt error

OpenSSL::TestPKCS12#test_create_with_chain_decode:
OpenSSL::PKCS12::PKCS12Error: encrypt error

OpenSSL::TestPKCS12#test_create_with_itr:
OpenSSL::PKCS12::PKCS12Error: encrypt error

OpenSSL::TestPKCS12#test_create_with_mac_itr:
OpenSSL::PKCS12::PKCS12Error: encrypt error

OpenSSL::TestX509Certificate#test_sign_and_verify:
OpenSSL::X509::CertificateError: unknown message digest algorithm

OpenSSL::TestX509Request#test_sign_and_verify:
OpenSSL::X509::RequestError: unknown message digest algorithm

(numerous tests)
/var/lib/mock/rhel-7-x86_64/root/builddir/build/BUILD/ruby-2.1.0/lib/rubygems/test_case.rb:1329:in `initialize': Neither PUB key nor PRIV key: nested asn1 error (OpenSSL::PKey::RSAError)

TestDigest::TestMD5#test_alignment = md5_dgst.c(80): OpenSSL internal error, assertion failed: Digest MD5 forbidden in FIPS mode!

TC_HMAC_MD5#test_hexdigest = md5_dgst.c(80): OpenSSL internal error, assertion failed: Digest MD5 forbidden in FIPS mode!

TestWEBrickHTTPAuth#test_digest_auth = md5_dgst.c(80): OpenSSL internal error, assertion failed: Digest MD5 forbidden in FIPS mode!

Persist in 230p0

TestString#test_crypt:
Errno::EPERM: Operation not permitted - crypt

TestString2#test_crypt:
Errno::EPERM: Operation not permitted - crypt

TestXMLRPC::Test_Webrick#test_client_server:
RuntimeError: HTTP-Error: 500 Internal Server Error

TestWEBrickHTTPAuth#test_basic_auth2
/builddir/build/BUILD/ruby-2.3.0/lib/webrick/httpauth/basicauth.rb:45:in `crypt': Operation not permitted - crypt (Errno::EPERM)

/builddir/build/BUILD/ruby-2.3.0/test/lib/minitest/unit.rb:201:in `assert': webrick log doesn't have expected error: /ERROR Basic WEBrick's realm: webrick: password unmatch./ (MiniTest::Assertion)

#36 - 11/10/2017 04:42 AM - rhenium (Kazuki Yamaguchi)

- Status changed from Assigned to Open

- Assignee deleted (7150)

(Removing assignee)

Can this be closed?

#37 - 11/07/2018 04:00 PM - jaruga (Jun Aruga)

@rhenium (Kazuki Yamaguchi) I think we can close this ticket.
Thanks for reminding us.
I do not see the issue on the fips mode.
I could pass the tests of trunk ruby with openssl 1.0.2 fips mode.

Right now the OpenSSL 1.1.1 does not support the building with fips mode.
But next release of OpenSSL 1.1 might support it. [1]

To keep green for the case of fips mode, and to prepare the future's release of OpenSSL 1.1 to support it, I proposed to add a case of OpenSSL 1.0.2 with fips mode to Travis CI or RubyCI or ruby/openssl. [2]

Or if we might create VM on RubyCI. I found the way for Fedora [3]. But I could not find for Ubuntu [4]

[1] https://github.com/openssl/openssl/issues/7582
[2] https://github.com/ruby/ruby/pull/2007
[3] https://www.dogtagpki.org/wiki/Enabling_FIPS_Mode_on_Fedora
[4] https://blog.ubuntu.com/2017/12/13/fips-140-2-certified-modules-for-ubuntu-16-04-lts

Files

output.txt	114 KB	08/28/2012	vo.x (Vit Ondruch)
output-r36887.txt	48.6 KB	09/04/2012	vo.x (Vit Ondruch)
output-r38509.txt	44.3 KB	12/22/2012	vo.x (Vit Ondruch)
output-200p353.txt	39.5 KB	01/30/2014	vo.x (Vit Ondruch)
output-210p0.txt	473 KB	01/30/2014	vo.x (Vit Ondruch)
output-230p0.txt	17 KB	06/20/2016	pvalena (Pavel Valena)