Ruby master - Bug #4550

Loading an RSA public key during an HTTPS connection corrupts the connection

04/04/2011 05:20 AM - drbrain (Eric Hodel)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 1.9.3dev (2011-03-30 trunk 31213) [x86_64-darwin10.6.0]	**Backport:**	

Description

=begin
The attached file creates an HTTPS connection to gmail.com then loads an RSA public key.

If a private key is loaded the error does not reproduce.

Loading of the public key corrupts the HTTPS connection resulting in the following error:

SSL_read:: no start line (OpenSSL::SSL::SSLError)

full output:

```
$ ruby19 -v -Ilib t.rb
ruby 1.9.3dev (2011-03-30 trunk 31213) [x86_64-darwin10.6.0]
opening connection to www.gmail.com...
opened
<- "GET / HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Ruby\r\nHost: "
-> "HTTP/1.1 301 Moved Permanently\r\n"
-> "Location: https://mail.google.com/mail/\r\n"
-> "Content-Type: text/html; charset=UTF-8\r\n"
-> "X-Content-Type-Options: nosniff\r\n"
-> "Date: Sun, 03 Apr 2011 20:15:44 GMT\r\n"
-> "Expires: Tue, 03 May 2011 20:15:44 GMT\r\n"
-> "Server: sffe\r\n"
-> "Content-Length: 226\r\n"
-> "X-XSS-Protection: 1; mode=block\r\n"
-> "Cache-Control: public, max-age=2592000\r\n"
-> "Age: 123\r\n"
-> "\r\n"
reading 226 bytes...
-> ""
-> "\n301 Moved\n301 Moved\nThe document has moved\nhere.\r\n\r\n"
read 226 bytes
Conn keep-alive
<- "GET / HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Ruby\r\nHost: "
Conn close because of error SSL_read:: no start line
/usr/local/lib/ruby/1.9.1/openssl/buffering.rb:174:in sysread_nonblock': SSL_read:: no start line (OpenSSL::SSL::SSLError)
from /usr/local/lib/ruby/1.9.1/openssl/buffering.rb:174:inread_nonblock'
from /usr/local/lib/ruby/1.9.1/net/protocol.rb:139:in rbuf_fill'
from /usr/local/lib/ruby/1.9.1/net/protocol.rb:120:inreaduntil'
from /usr/local/lib/ruby/1.9.1/net/protocol.rb:130:in readline'
from /usr/local/lib/ruby/1.9.1/net/http.rb:2517:inread_status_line'
from /usr/local/lib/ruby/1.9.1/net/http.rb:2506:in read_new'
from /usr/local/lib/ruby/1.9.1/net/http.rb:1296:intransport_request'
from /usr/local/lib/ruby/1.9.1/net/http.rb:1271:in request'
from t.rb:18:inblock in '
from /usr/local/lib/ruby/1.9.1/net/http.rb:732:in start'
from t.rb:11:in'
```

This bug was originally reported on mechanize: https://github.com/tenderlove/mechanize/issues#issue/27
=end

Associated revisions

Revision e61d269f - 04/06/2011 02:44 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_rsa.c (ossl_rsa_initialize): pop pushed error after each try of reading. fixes #4550

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@31242 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31242 - 04/06/2011 02:44 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_rsa.c (ossl_rsa_initialize): pop pushed error after each try of reading. fixes #4550

Revision 31242 - 04/06/2011 02:44 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_rsa.c (ossl_rsa_initialize): pop pushed error after each try of reading. fixes #4550

Revision 31242 - 04/06/2011 02:44 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_rsa.c (ossl_rsa_initialize): pop pushed error after each try of reading. fixes #4550

Revision 31242 - 04/06/2011 02:44 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_rsa.c (ossl_rsa_initialize): pop pushed error after each try of reading. fixes #4550

Revision 31242 - 04/06/2011 02:44 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_rsa.c (ossl_rsa_initialize): pop pushed error after each try of reading. fixes #4550

Revision 31242 - 04/06/2011 02:44 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_rsa.c (ossl_rsa_initialize): pop pushed error after each try of reading. fixes #4550

Revision d5b1fde5 - 04/06/2011 06:14 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_dh.c (ossl_dh_initialize):
  pop pushed error after each try of reading. fixes #4550

- ext/openssl/ossl_pkey_dsa.c (ossl_dsa_initialize): ditto.

- ext/openssl/ossl_pkey_ec.c (ossl_ec_initialize): ditto.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@31244 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31244 - 04/06/2011 06:14 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_dh.c (ossl_dh_initialize):
  pop pushed error after each try of reading. fixes #4550

- ext/openssl/ossl_pkey_dsa.c (ossl_dsa_initialize): ditto.

- ext/openssl/ossl_pkey_ec.c (ossl_ec_initialize): ditto.

Revision 31244 - 04/06/2011 06:14 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_dh.c (ossl_dh_initialize):
  pop pushed error after each try of reading. fixes #4550

- ext/openssl/ossl_pkey_dsa.c (ossl_dsa_initialize): ditto.
- ext/openssl/ossl_pkey_ec.c (ossl_ec_initialize): ditto.

Revision 31244 - 04/06/2011 06:14 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_dh.c (ossl_dh_initialize):
  pop pushed error after each try of reading. fixes #4550
- ext/openssl/ossl_pkey_dsa.c (ossl_dsa_initialize): ditto.
- ext/openssl/ossl_pkey_ec.c (ossl_ec_initialize): ditto.

Revision 31244 - 04/06/2011 06:14 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_dh.c (ossl_dh_initialize):
  pop pushed error after each try of reading. fixes #4550
- ext/openssl/ossl_pkey_dsa.c (ossl_dsa_initialize): ditto.
- ext/openssl/ossl_pkey_ec.c (ossl_ec_initialize): ditto.

Revision 31244 - 04/06/2011 06:14 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_dh.c (ossl_dh_initialize):
  pop pushed error after each try of reading. fixes #4550
- ext/openssl/ossl_pkey_dsa.c (ossl_dsa_initialize): ditto.
- ext/openssl/ossl_pkey_ec.c (ossl_ec_initialize): ditto.

Revision 31244 - 04/06/2011 06:14 AM - naruse (Yui NARUSE)

- ext/openssl/ossl_pkey_dh.c (ossl_dh_initialize):
  pop pushed error after each try of reading. fixes #4550
- ext/openssl/ossl_pkey_dsa.c (ossl_dsa_initialize): ditto.
- ext/openssl/ossl_pkey_ec.c (ossl_ec_initialize): ditto.

Revision dd11a58b - 04/12/2011 09:08 AM - kouji (Kouji Takao)

- ext/readline/extconf.rb: --disable-libedit to disable libedit. fixes #4550

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@31265 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31265 - 04/12/2011 09:08 AM - kouji (Kouji Takao)

- ext/readline/extconf.rb: --disable-libedit to disable libedit. fixes #4550

Revision 31265 - 04/12/2011 09:08 AM - kouji (Kouji Takao)

- ext/readline/extconf.rb: --disable-libedit to disable libedit. fixes #4550

Revision 31265 - 04/12/2011 09:08 AM - kouji (Kouji Takao)

- ext/readline/extconf.rb: --disable-libedit to disable libedit. fixes #4550

Revision 31265 - 04/12/2011 09:08 AM - kouji (Kouji Takao)

- ext/readline/extconf.rb: --disable-libedit to disable libedit. fixes #4550

Revision 31265 - 04/12/2011 09:08 AM - kouji (Kouji Takao)

- ext/readline/extconf.rb: --disable-libedit to disable libedit. fixes #4550

Revision 31265 - 04/12/2011 09:08 AM - kouji (Kouji Takao)

- ext/readline/extconf.rb: --disable-libedit to disable libedit. fixes #4550

Revision 1dd5d8e4 - 05/29/2011 10:49 PM - yugui (Yuki Sonoda)

merges r31242 from trunk into ruby_1_9_2.

- ext/openssl/ossl_pkey_rsa.c (ossl_rsa_initialize): pop pushed error after each try of reading. fixes #4550

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_2@31795 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61ce0127 - 05/29/2011 10:49 PM - yugui (Yuki Sonoda)

merges r31244 from trunk into ruby_1_9_2.

- ext/openssl/ossl_pkey_dh.c (ossl_dh_initialize):
  pop pushed error after each try of reading. fixes #4550
- ext/openssl/ossl_pkey_dsa.c (ossl_dsa_initialize): ditto.
- ext/openssl/ossl_pkey_ec.c (ossl_ec_initialize): ditto.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_2@31796 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 04/06/2011 01:03 PM - naruse (Yui NARUSE)

- Status changed from Open to Closed

- % Done changed from 0 to 100

=begin
This issue was solved with changeset r31242.
Eric, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

=end

Files

t.rb	367 Bytes	04/04/2011	drbrain (Eric Hodel)