Ruby trunk - Bug #9053

SSL Issue with Ruby 2.0.0

10/25/2013 06:24 PM - tisba (Sebastian Cohnen)

Status:	Third Party's Issue		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:	ruby 2.0.0p247 (2013-06-27 revision 41674) [x86_64-darwin13.0.0]	**Backport:**	

Description

=begin
Steps to reproduce:

ruby -rnet/http -e 'Net::HTTP.get(URI("https://stormforger.com"));'

results in:

/Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:918:in connect': SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify failed (OpenSSL::SSL::SSLError)
from /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:918:inblock in connect'
from /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/timeout.rb:52:in timeout'
from /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:918:inconnect'
from /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:862:in do_start'
from /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:851:instart'
from /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:582:in start'
from /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:477:inget_response'
from /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:454:in get'
from -e:1:in'

But I expected no output from the program.

Running the same code with Ruby 1.8.7 or 1.9.3 causes no problems. I was able to reproduce this issue with OS X 10.8.5 as well as with 10.9. Interestingly OS X 10.9's system ruby ((({ruby 2.0.0p247 (2013-06-27 revision 41674) [universal.x86_64-darwin13]}))) does not have the issue. I appended the output of (({otool -L})) to look for the used OpenSSL lib. Apple's ruby obviously uses Apples own OpenSSL lib. 1.9.3 and 2.0.0 use the same OpenSSL lib, but only 2.0.0 fails on my test.

ruby-head ((({ruby 2.1.0dev (2013-10-24 trunk 43413) [x86_64-darwin13.0.0]}))) is also affected.

Just FYI: I initially reported the issue to RVM[0], but it appears to be not really RVM related.

[0] https://github.com/wayneeseguin/rvm/issues/2315

[1] Output of otool for various tested Rubies:

((*1.9.3-p448*))

$ find ~/.rvm/rubies/ruby-1.9.3-p448 -name openssl.bundle | xargs otool -L
/Users/basti/.rvm/rubies/ruby-1.9.3-p448/lib/ruby/1.9.1/x86_64-darwin13.0.0/openssl.bundle:
/Users/basti/.rvm/rubies/ruby-1.9.3-p448/lib/libruby.1.9.1.dylib (compatibility version 1.9.1, current version 1.9.1)
/usr/local/opt/openssl/lib/libssl.1.0.0.dylib (compatibility version 1.0.0, current version 1.0.0)
/usr/local/opt/openssl/lib/libcrypto.1.0.0.dylib (compatibility version 1.0.0, current version 1.0.0)
/usr/lib/libz.1.dylib (compatibility version 1.0.0, current version 1.2.5)
/usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1197.1.1)
/usr/lib/libobjc.A.dylib (compatibility version 1.0.0, current version 228.0.0)

((*2.0.0-p247*))

$ find ~/.rvm/rubies/ruby-2.0.0-p247 -name openssl.bundle | xargs otool -L
/Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/x86_64-darwin13.0.0/openssl.bundle:
/usr/local/opt/openssl/lib/libssl.1.0.0.dylib (compatibility version 1.0.0, current version 1.0.0)
/usr/local/opt/openssl/lib/libcrypto.1.0.0.dylib (compatibility version 1.0.0, current version 1.0.0)

/usr/lib/libz.1.dylib (compatibility version 1.0.0, current version 1.2.5)
/Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/libruby.2.0.0.dylib (compatibility version 2.0.0, current version 2.0.0)
/usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1197.1.1)
/usr/lib/libobjc.A.dylib (compatibility version 1.0.0, current version 228.0.0)

((*2.0.0-p247 System Ruby*))

$ find /usr/lib/ruby/2.0.0/ -name openssl.bundle | xargs otool -L
/usr/lib/ruby/2.0.0//universal-darwin13/openssl.bundle:
/System/Library/Frameworks/Ruby.framework/Versions/2.0/usr/lib/libruby.2.0.0.dylib (compatibility version 2.0.0, current version 2.0.0)
/usr/lib/libssl.0.9.8.dylib (compatibility version 0.9.8, current version 50.0.0)
/usr/lib/libcrypto.0.9.8.dylib (compatibility version 0.9.8, current version 50.0.0)
/usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1197.1.1)
/usr/lib/libobjc.A.dylib (compatibility version 1.0.0, current version 228.0.0)

=end

History

#1 - 10/26/2013 05:59 AM - drbrain (Eric Hodel)

- Category set to ext/openssl

- Status changed from Open to Rejected

- Assignee set to drbrain (Eric Hodel)

You need to install certificates when using non-platform OpenSSL on OS X. Your certificates should be installed here:

ruby -ropenssl -e 'puts OpenSSL::X509::DEFAULT_CERT_FILE'

There are instructions on how to install them for RVM:

http://rvm.io/support/fixing-broken-ssl-certificates

#2 - 10/26/2013 10:30 AM - mpapis (Michal Papis)

=begin
as per the RVM ticket
rvm osx-ssl-certs update all
was used, I do not think this one is missing certificates, any steps to help debug it?
=end

#3 - 10/26/2013 11:12 AM - drbrain (Eric Hodel)

- Status changed from Rejected to Assigned

- Assignee changed from drbrain (Eric Hodel) to MartinBosslet (Martin Bosslet)

Ah, I missed that.

Maybe Martin knows, I have assigned the issue to him.

#4 - 10/26/2013 10:37 PM - chittoor (Rajesh Malepati)

tisba (Sebastian Cohnen) wrote:

> =begin
> Steps to reproduce:
>
> ruby -rnet/http -e 'Net::HTTP.get(URI("https://stormforger.com"));'
>
> results in:
>
> /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:918:in `connect': SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify failed (OpenSSL::SSL::SSLError)

Your certificate chain is incomplete.
Serve "StartCom Class 1 Primary Intermediate Server CA" certificate along with your server certificate.

#5 - 10/28/2013 04:56 PM - tisba (Sebastian Cohnen)

chittoor (Rajesh Malepati) wrote:

> tisba (Sebastian Cohnen) wrote:
>
> > =begin
> > Steps to reproduce:
> >
> > ruby -rnet/http -e 'Net::HTTP.get(URI("https://stormforger.com"));'
> >
> > results in:
> >
> > /Users/basti/.rvm/rubies/ruby-2.0.0-p247/lib/ruby/2.0.0/net/http.rb:918:in `connect': SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify failed (OpenSSL::SSL::SSLError)
>
> Your certificate chain is incomplete.
> Serve "StartCom Class 1 Primary Intermediate Server CA" certificate along with your server certificate.

Okay thanks, I'll take a look.

But this doesn't really explain, why only Ruby 2.0 is affected, or does it?

#6 - 10/29/2013 03:07 AM - chittoor (Rajesh Malepati)

tisba (Sebastian Cohnen) wrote:

> chittoor (Rajesh Malepati) wrote:
>
> > Your certificate chain is incomplete.
> > Serve "StartCom Class 1 Primary Intermediate Server CA" certificate along with your server certificate.
>
> Okay thanks, I'll take a look.
>
> But this doesn't really explain, why only Ruby 2.0 is affected, or does it?

Are you sure it's just Ruby 2.0? openssl doesn't attempt to download missing certificates.
Browsers on the other hand, look at 'Authority Information Access' extension in the certificate to download additional certificates.

#7 - 11/02/2013 08:46 AM - mpapis (Michal Papis)

I think it can be closed as per https://github.com/wayneeseguin/rvm/issues/2315#issuecomment-27198136 - adding the missing certificate fixes the problem

#8 - 11/02/2013 09:19 AM - davispuh (Dāvis Mosāns)

=begin
I've same problem on Windows 8 using Ruby 2.0.0-p247 (x86) from ((), no RVM
=end

#9 - 11/02/2013 09:24 AM - davispuh (Dāvis Mosāns)

=begin
On Linux it works fine, but on Windows:

N:\Projects>ruby -rnet/http -e 'Net::HTTP.get(URI("https://google.com"));'
P:/Ruby200/lib/ruby/2.0.0/net/http.rb:918:in connect': SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify failed (OpenSSL::SSL::SSLError)
from P:/Ruby200/lib/ruby/2.0.0/net/http.rb:918:inblock in connect'
from P:/Ruby200/lib/ruby/2.0.0/timeout.rb:52:in timeout'
from P:/Ruby200/lib/ruby/2.0.0/net/http.rb:918:inconnect'
from P:/Ruby200/lib/ruby/2.0.0/net/http.rb:862:in do_start'
from P:/Ruby200/lib/ruby/2.0.0/net/http.rb:851:instart'
from P:/Ruby200/lib/ruby/2.0.0/net/http.rb:582:in start'
from P:/Ruby200/lib/ruby/2.0.0/net/http.rb:477:inget_response'
from P:/Ruby200/lib/ruby/2.0.0/net/http.rb:454:in get'
from -e:1:in'
=end

#10 - 11/04/2013 09:47 AM - MartinBosslet (Martin Bosslet)

Thanks everyone for contributing, I'm sorry I couldn't look into it any sooner. Special thanks to Rajesh for finding the issue!

@Sebastian: Adding the missing certificate in the chain fixed the issue for you?

@Dāvis: What does

openssl version -a

print for you? At the very end, there should be an entry similar to

OPENSSLDIR: "/etc/pki/tls"

What directory does the command display? Does it exist, and if yes, what files are in there?

#11 - 11/04/2013 11:42 AM - luislavena (Luis Lavena)

=begin
davispuh (Dāvis Mosāns): OpenSSL in Windows do not come with support for Windows certificate storage, so it cannot connect to HTTPS servers without a valid certificate bundle.

You need to use ((|SSL_CERT_FILE|)) environment variable and set to the path to a curl CA cert bundle.

As for RubyGems, I recommend updating to the latest version of the version you're using (e.g. 2.1.10 for 2.1.x, 2.0.13 for 2.0.x and 1.8.28 for 1.8.x)

You can follow the installation instructions here:

http://rubygems.rubyforge.org/rubygems-update/UPGRADING_rdoc.html

=end

#12 - 11/05/2013 05:40 PM - tisba (Sebastian Cohnen)

MartinBosslet (Martin Bosslet) wrote:

> Thanks everyone for contributing, I'm sorry I couldn't look into it any sooner. Special thanks to Rajesh for finding the issue!
>
> @Sebastian: Adding the missing certificate in the chain fixed the issue for you?

Yes, I added the intermediate certificate to be served as well and this fixed the issue for me.

#13 - 11/05/2013 05:54 PM - tisba (Sebastian Cohnen)

chittoor (Rajesh Malepati) wrote:

> tisba (Sebastian Cohnen) wrote:
>
> > chittoor (Rajesh Malepati) wrote:
> >
> > > Your certificate chain is incomplete.
> > > Serve "StartCom Class 1 Primary Intermediate Server CA" certificate along with your server certificate.
> >
> > Okay thanks, I'll take a look.
> >
> > But this doesn't really explain, why only Ruby 2.0 is affected, or does it?
>
> Are you sure it's just Ruby 2.0? openssl doesn't attempt to download missing certificates.
> Browsers on the other hand, look at 'Authority Information Access' extension in the certificate to download additional certificates.

I just removed the intermediate certificate again from the server to test it again. I noticed that Ruby 1.9.3 (and 1.8.7) does not seem to verify the SSL certificate by default (OpenSSL::SSL::VERIFY_NONE). This code fails for all Rubies (1.8.7, 1.9.3 and 2.0.0) with the missing intermediate certificate:

```
require "net/http"
http = Net::HTTP.new("stormforger.com", 443)
http.use_ssl = true
http.verify_mode = OpenSSL::SSL::VERIFY_PEER
request = Net::HTTP::Get.new("/")
response = http.request(request)
```

results in:

OpenSSL::SSL::SSLError: SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify failed

#14 - 09/13/2015 03:11 AM - zzak (Zachary Scott)

- Assignee changed from MartinBosslet (Martin Bosslet) to openssl

#15 - 07/02/2016 04:39 AM - rhenium (Kazuki Yamaguchi)

- Backport deleted (1.9.3: UNKNOWN, 2.0.0: UNKNOWN)

- Status changed from Assigned to Third Party's Issue

Closing as the issue was resolved.