Ruby - Bug #10910

NoMethodError when opening SSL connection with OpenSSL::SSL::VERIFY_PEER set and anonymous ciphers allowed

02/26/2015 10:54 PM - Sinjo (Chris Sinjakli)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.3.0dev	**Backport:**	2.0.0: REQUIRED, 2.1: DONE, 2.2: DONE

Description

When establishing an SSL connection with peer verification enabled, if the list of allowed ciphers includes an anonymous cipher, and negotiation with the server results in that cipher being used, a NoMethodError is raised with a stack trace like:

```
/Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/openssl/ssl.rb:99:in `verify_certificate_identity': undef
ined method `extensions' for nil:NilClass (NoMethodError)
        from /Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/openssl/ssl.rb:156:in `post_connection_check
'
        from /Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/net/http.rb:922:in `connect'
        from /Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/net/http.rb:863:in `do_start'
        from /Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/net/http.rb:852:in `start'
        from ../test_ssl.rb:4:in `<main>'
```

This is because no certificate is returned when using an anonymous cipher, while the verification code which runs when OpenSSL::SSL::VERIFY_PEER is set expects one to be present.

I've attached a patch which fixes this. Let me know if there's anything you'd like me to change (happy to refactor, or alter the approach).

This behaviour is present in 2.0, 2.1, and 2.2.

Associated revisions

Revision dc9ca079bbd37e9e6ab5caed48a665aa616aa2a1 - 07/27/2015 06:29 PM - tenderlovemaking (Aaron Patterson)

- ext/openssl/lib/openssl/ssl.rb (module OpenSSL): raise a more helpful exception when verifying the peer connection and an anonymous cipher has been selected. [ruby-core:68330] [Bug #10910] Thanks to Chris Sinjakli chris@sinjakli.co.uk for the patch.
- test/openssl/test_ssl.rb (class OpenSSL): test for change

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@51409 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision dc9ca079 - 07/27/2015 06:29 PM - tenderlovemaking (Aaron Patterson)

- ext/openssl/lib/openssl/ssl.rb (module OpenSSL): raise a more helpful exception when verifying the peer connection and an anonymous cipher has been selected. [ruby-core:68330] [Bug #10910] Thanks to Chris Sinjakli chris@sinjakli.co.uk for the patch.
- test/openssl/test_ssl.rb (class OpenSSL): test for change

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@51409 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 04a567fb4bb650b2b5c94851db6b59bd460e7da1 - 08/12/2015 03:16 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 51409,51453: [Backport #10910]

```
    * ext/openssl/lib/openssl/ssl.rb (module OpenSSL): raise a more
      helpful exception when verifying the peer connection and an
      anonymous cipher has been selected. [ruby-core:68330] [Bug #10910]
      Thanks to Chris Sinjakli <chris@sinjakli.co.uk> for the patch.

    * test/openssl/test_ssl.rb (class OpenSSL): test for change

    * .travis.yml: update libssl before running tests.
      Thanks to Chris Sinjakli <chris@sinjakli.co.uk> for figuring out the
      travis settings!
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@51554 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 04a567fb - 08/12/2015 03:16 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 51409,51453: [Backport #10910]

```
    * ext/openssl/lib/openssl/ssl.rb (module OpenSSL): raise a more
      helpful exception when verifying the peer connection and an
      anonymous cipher has been selected. [ruby-core:68330] [Bug #10910]
      Thanks to Chris Sinjakli <chris@sinjakli.co.uk> for the patch.

    * test/openssl/test_ssl.rb (class OpenSSL): test for change

    * .travis.yml: update libssl before running tests.
      Thanks to Chris Sinjakli <chris@sinjakli.co.uk> for figuring out the
      travis settings!
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@51554 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision d3cd7b4813dcaf4022d8d70b8dd9f2bd17812d56 - 08/17/2015 08:30 AM - U.Nakamura

merge revision(s) 51409,51453: [Backport #10910]

```
    * ext/openssl/lib/openssl/ssl.rb (module OpenSSL): raise a more
      helpful exception when verifying the peer connection and an
      anonymous cipher has been selected. [ruby-core:68330] [Bug #10910]
      Thanks to Chris Sinjakli <chris@sinjakli.co.uk> for the patch.

    * test/openssl/test_ssl.rb (class OpenSSL): test for change

    * .travis.yml: update libssl before running tests.
      Thanks to Chris Sinjakli <chris@sinjakli.co.uk> for figuring out the
      travis settings!
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@51608 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision d3cd7b48 - 08/17/2015 08:30 AM - U.Nakamura

merge revision(s) 51409,51453: [Backport #10910]

```
    * ext/openssl/lib/openssl/ssl.rb (module OpenSSL): raise a more
      helpful exception when verifying the peer connection and an
      anonymous cipher has been selected. [ruby-core:68330] [Bug #10910]
      Thanks to Chris Sinjakli <chris@sinjakli.co.uk> for the patch.

    * test/openssl/test_ssl.rb (class OpenSSL): test for change

    * .travis.yml: update libssl before running tests.
      Thanks to Chris Sinjakli <chris@sinjakli.co.uk> for figuring out the
      travis settings!
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@51608 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 03/26/2015 07:36 AM - zzak (zzak _)

- Status changed from Open to Assigned

- Assignee set to 7150

#2 - 07/14/2015 11:20 PM - Sinjo (Chris Sinjakli)

Just wondering what the status is on this one. I noticed it got assigned to the openssl group a few months back, but there's been no word since then.

#3 - 07/23/2015 10:10 PM - tenderlovemaking (Aaron Patterson)

- Status changed from Assigned to Feedback

Hi,

When I apply just the test, it doesn't fail. Are you sure the bug is still present? If it's still present, can you make a test that fails without changes to the implementation?

#4 - 07/25/2015 02:26 PM - Sinjo (Chris Sinjakli)

Just rebased against trunk, and the test still fails on my machine if I remove the changes to ext/openssl/lib/openssl/ssl.rb.

For a little more context, I'm running the test on OS X Yosemite, linking against OpenSSL from Homebrew (version OpenSSL 1.0.2d 9 Jul 2015). I originally ran into this on Ubuntu 12.04, but I don't have that machine running any more, so I can't check the OpenSSL version.

One thing I just thought of is that ADH-AES256-GCM-SHA384 might not be available in all versions of OpenSSL. I'm not sure what would happen in that case, as I don't provide a fallback cipher in the tests with use_anon_cipher: true.

#5 - 07/26/2015 04:07 PM - tenderlovemaking (Aaron Patterson)

I see. I'm not sure what I did wrong because it seems to be behaving correctly now. Maybe I was running an older version of openssl. Anyway, the patch looks good to me. I just wish there was an easier way to get a list of the default ciphers other than allocating a new SSLContext object. I'll poke around and see what I can find, but other than that the patch looks good to me.

#6 - 07/26/2015 04:07 PM - tenderlovemaking (Aaron Patterson)

- Status changed from Feedback to Assigned

#7 - 07/27/2015 06:29 PM - Anonymous

- Status changed from Assigned to Closed

Applied in changeset r51409.

- ext/openssl/lib/openssl/ssl.rb (module OpenSSL): raise a more helpful exception when verifying the peer connection and an anonymous cipher has been selected. [ruby-core:68330] [Bug #10910] Thanks to Chris Sinjakli chris@sinjakli.co.uk for the patch.
- test/openssl/test_ssl.rb (class OpenSSL): test for change

#8 - 07/30/2015 09:17 AM - nobu (Nobuyoshi Nakada)

- Status changed from Closed to Open

This has failed on travis.

https://travis-ci.org/ruby/ruby/builds/72882783

#9 - 07/30/2015 03:18 PM - tenderlovemaking (Aaron Patterson)

Thanks, I'm taking a look.

On Thu, Jul 30, 2015 at 09:17:38AM +0000, nobu@ruby-lang.org wrote:

> Issue #10910 has been updated by Nobuyoshi Nakada.
>
> Status changed from Closed to Open
>
> This has failed on travis.
>
> https://travis-ci.org/ruby/ruby/builds/72882783
>
> ---
>
> Bug #10910: NoMethodError when opening SSL connection with OpenSSL::SSL::VERIFY_PEER set and anonymous ciphers allowed
> https://bugs.ruby-lang.org/issues/10910#change-53613
>
> - Author: Chris Sinjakli

- Status: Open
- Priority: Normal
- Assignee: openssl
- ruby -v: ruby 2.3.0dev
- Backport: 2.0.0: REQUIRED, 2.1: REQUIRED, 2.2: REQUIRED

When establishing an SSL connection with peer verification enabled, if the list of allowed ciphers includes an anonymous cipher, and negotiation with the server results in that cipher being used, a NoMethodError is raised with a stack trace like:

```
/Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/openssl/ssl.rb:99:in `verify_certificate_identity': undefined met
hod `extensions' for nil:NilClass (NoMethodError)
        from /Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/openssl/ssl.rb:156:in `post_connection_check'
        from /Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/net/http.rb:922:in `connect'
        from /Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/net/http.rb:863:in `do_start'
        from /Users/sinjo/rubies/2.1.3/lib/ruby/2.1.0/net/http.rb:852:in `start'
        from ../test_ssl.rb:4:in `<main>'
```

This is because no certificate is returned when using an anonymous cipher, while the verification code which runs when OpenSSL::SSL::VERIFY_PEER is set expects one to be present.

I've attached a patch which fixes this. Let me know if there's anything you'd like me to change (happy to refactor, or alter the approach).

This behaviour is present in 2.0, 2.1, and 2.2.

---Files--------------------------------
ssl_verify.patch (2.71 KB)

--
https://bugs.ruby-lang.org/

--
Aaron Patterson
http://tenderlovemaking.com/

#10 - 07/31/2015 11:01 AM - Sinjo (Chris Sinjakli)

- File update_libssl_on_travis.patch added

Turns out Travis ships an old, apparently broken version of libssl. I've attached a patch which updates it before running the build. You can see the patch running on this build: https://travis-ci.org/Sinjo/ruby/builds/73534479

#11 - 07/31/2015 03:03 PM - tenderlovemaking (Aaron Patterson)

- Status changed from Open to Closed

Thanks. I've applied the patch and the build is green now.

#12 - 08/12/2015 03:17 PM - nagachika (Tomoyuki Chikanaga)

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

r51409 and r51453 were backported into ruby_2_2 branch at r51554.

#13 - 08/17/2015 08:30 AM - usa (Usaku NAKAMURA)

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

ruby_2_1 r51608 merged revision(s) 51409,51453.
note: changed a little to get rid of conflicts.

Files

ssl_verify.patch	2.71 KB	02/26/2015	Sinjo (Chris Sinjakli)
update_libssl_on_travis.patch	821 Bytes	07/31/2015	Sinjo (Chris Sinjakli)