Backport21 - Backport #9640

Please backport SSL fixes to 2.1

03/15/2014 11:21 AM - zeha (Christian Hofstaedtler)

Status:	Closed	
Priority:	Normal	
Assignee:	nagachika (Tomoyuki Chikanaga)	

Description

Please backport the fixes for issue #9424 to 2.1.

https://bugs.ruby-lang.org/projects/ruby-trunk/repository/revisions/45274/diff/ext/openssl/lib/openssl/ssl.rb

Related issues:

Related to Ruby master - Feature #9613: Warn about unsafe ossl ciphers	**Open**	
Related to Ruby master - Bug #9424: ruby 1.9 & 2.x has insecure SSL/TLS clien...	**Closed**	**01/17/2014**

Associated revisions

Revision c8137d67 - 10/22/2014 02:14 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r45274,r45278,r45280,r48097: [Backport #9424] [Backport #9640]

```
    * lib/openssl/ssl.rb: Explicitly whitelist the default
      SSL/TLS ciphers. Forbid SSLv2 and SSLv3, disable
      compression by default.
      Reported by Jeff Hodges.
      [ruby-core:59829] [Bug #9424]

    * test/openssl/test_ssl.rb: Reuse TLS default options from
      OpenSSL::SSL::SSLContext::DEFAULT_PARAMS.

    * ext/openssl/lib/openssl/ssl.rb (DEFAULT_PARAMS): override
      options even if OpenSSL::SSL::OP_NO_SSLv3 is not defined.
      this is pointed out by Stephen Touset. [ruby-core:65711] [Bug #9424]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@48098 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 48098 - 10/22/2014 02:14 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r45274,r45278,r45280,r48097: [Backport #9424] [Backport #9640]

```
* lib/openssl/ssl.rb: Explicitly whitelist the default
  SSL/TLS ciphers. Forbid SSLv2 and SSLv3, disable
  compression by default.
  Reported by Jeff Hodges.
  [ruby-core:59829] [Bug #9424]

* test/openssl/test_ssl.rb: Reuse TLS default options from
  OpenSSL::SSL::SSLContext::DEFAULT_PARAMS.

* ext/openssl/lib/openssl/ssl.rb (DEFAULT_PARAMS): override
  options even if OpenSSL::SSL::OP_NO_SSLv3 is not defined.
  this is pointed out by Stephen Touset. [ruby-core:65711] [Bug #9424]
```

History

#1 - 03/16/2014 03:08 AM - hsbt (Hiroshi SHIBATA)

It seems to break backward compatibility.

#2 - 03/16/2014 04:06 AM - zzak (Zachary Scott)

- Status changed from Open to Rejected

Please Don't report issues here.

Also, there is already a ticket to discuss this patch in #9613

#3 - 03/17/2014 01:39 PM - hsbt (Hiroshi SHIBATA)

- Status changed from Rejected to Open

> zzak

You shouldn't change status of backport issue by yourself. It's branch maintainer's work.

#4 - 03/17/2014 06:54 PM - naruse (Yui NARUSE)

- Related to Feature #9613: Warn about unsafe ossl ciphers added

#5 - 03/17/2014 06:55 PM - naruse (Yui NARUSE)

- Related to Bug #9424: ruby 1.9 & 2.x has insecure SSL/TLS client defaults added

#6 - 03/17/2014 07:03 PM - naruse (Yui NARUSE)

Zachary Scott wrote:

> Please Don't report issues here.

If the ticket is really backport ticket, here is correct place;
and this ticket is actually a backport ticket.

#7 - 03/18/2014 04:53 AM - zzak (Zachary Scott)

Sorry for the misunderstanding, I think we should discuss it on trunk first.

Also, I don't believe the current patch (as-is) should be backported.

On Mar 17, 2014, at 7:09 PM, shibata.hiroshi@gmail.com wrote:

> Issue #9640 has been updated by Hiroshi SHIBATA.
>
> Status changed from Rejected to Open
>
> > zzak
>
> You shouldn't change status of backport issue by yourself. It's branch maintainer's work.
>
> ---
>
> Backport #9640: Please backport SSL fixes to 2.1
> https://bugs.ruby-lang.org/issues/9640#change-45837
>
> - Author: Christian Hofstaedtler
> - Status: Open
> - Priority: Normal
>
> # * Assignee:
>
> Please backport the fixes for issue #9424 to 2.1.
>
> https://bugs.ruby-lang.org/projects/ruby-trunk/repository/revisions/45274/diff/ext/openssl/lib/openssl/ssl.rb
>
> --
> http://bugs.ruby-lang.org/

#8 - 10/15/2014 06:15 AM - reed (Reed Loden)

Since the POODLE attack was released today (and is causing folks to generally disable SSLv3 everywhere), any possibility of getting the patch backported to a current stable release of Ruby so people can be protected against it and other problems?

#9 - 10/18/2014 05:50 PM - nagachika (Tomoyuki Chikanaga)

I thought before it cannot be backported because it seems to cause compatibility issues.
But now I feel the necessity of rethink about it according to the change of circumstance (ex. POODLE).

I think users can protect themselves via configuration or update OpenSSL itself, not the by ruby C extension library. Is it correct?

I think r45274 changes only default settings, so users who need SSLv3 or old ciphers have some workarounds, for example via Net::HTTP#ssl_version= or Net::HTTP#ciphers=). Is it correct?

#10 - 10/19/2014 03:54 AM - usa (Usaku NAKAMURA)

Tomoyuki Chikanaga wrote:

> But now I feel the necessity of rethink about it according to the change of circumstance (ex. POODLE).

I feel so, too.

> I think users can protect themselves via configuration or update OpenSSL itself, not the by ruby C extension library. Is it correct?

ext/openssl(/lib/openssl/ssl.rb) actually sets the default of chiphers, so changing them of OpenSSL itself is meaningless about us.
Am I wrong?

> I think r45274 changes only default settings, so users who need SSLv3 or old ciphers have some workarounds, for example via Net::HTTP#ssl_version= or Net::HTTP#ciphers=). Is it correct?

Since net/http does not have the interface to change the ciphers at the moment, available workaround should be a complex monkey patch, I guess.

#11 - 10/19/2014 02:27 PM - nagachika (Tomoyuki Chikanaga)

> > I think users can protect themselves via configuration or update OpenSSL itself, not the by ruby C extension library. Is it correct?
>
> ext/openssl(/lib/openssl/ssl.rb) actually sets the default of chiphers, so changing them of OpenSSL itself is meaningless about us.
> Am I wrong?

Thank you for pointing out that. It seems that I misunderstood about the point.
So I think we *should* backport the change.

> Since net/http does not have the interface to change the ciphers at the moment, available workaround should be a complex monkey patch, I guess.

Yes. But I think the workaround to do something potentially dangerous could be complicated. Users should know what they really to do.

#12 - 10/19/2014 03:10 PM - usa (Usaku NAKAMURA)

Tomoyuki Chikanaga wrote:

> Yes. But I think the workaround to do something potentially dangerous could be complicated. Users should know what they really to do.

agreed.

So, the way to do is:

- backport this patch
- say "if you have some trouble, revert this patch by yourself in your own risk"

#13 - 10/22/2014 01:34 PM - nagachika (Tomoyuki Chikanaga)

- Status changed from Open to Assigned

- Assignee set to nagachika (Tomoyuki Chikanaga)

OK, I'll handle this ticket.
And I filled the 'Backport' field of #9424 too.

#14 - 10/22/2014 02:15 PM - nagachika (Tomoyuki Chikanaga)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

Applied in changeset r48098.

merge revision(s) r45274,r45278,r45280,r48097: [Backport #9424] [Backport #9640]

```
* lib/openssl/ssl.rb: Explicitly whitelist the default
  SSL/TLS ciphers. Forbid SSLv2 and SSLv3, disable
  compression by default.
  Reported by Jeff Hodges.
  [ruby-core:59829] [Bug #9424]

* test/openssl/test_ssl.rb: Reuse TLS default options from
  OpenSSL::SSL::SSLContext::DEFAULT_PARAMS.

* ext/openssl/lib/openssl/ssl.rb (DEFAULT_PARAMS): override
  options even if OpenSSL::SSL::OP_NO_SSLv3 is not defined.
  this is pointed out by Stephen Touset. [ruby-core:65711] [Bug #9424]
```