

## Ruby - Feature #11524

### Use TLS 1.2 to default version of OpenSSL

09/12/2015 08:35 AM - hsbt (Hiroshi SHIBATA)

<b>Status:</b>	Closed	
<b>Priority:</b>	Normal	
<b>Assignee:</b>		
<b>Target version:</b>		
<b>Description</b> OpenSSL on trunk still use SSL version 3 with default option. but SSLv3 have some vulnerability.  I propose to use TLS 1.2 with default on OpenSSL library.  see original proposal: <a href="https://github.com/ruby/ruby/pull/873">https://github.com/ruby/ruby/pull/873</a>  In other side, HTTP/2 must be required TLS 1.2 protocol. We should change it before http client author put ctx.ssl_version = :TLSv1_2 every their code.  ref. <a href="https://http2.github.io/http2-spec/#TLSUsage">https://http2.github.io/http2-spec/#TLSUsage</a>		

#### Associated revisions

##### Revision 4b395bb4cecf23244617319a187391b7c885d864 - 10/08/2015 05:26 AM - zzak (zzak \_)

- ext/openssl/lib/openssl/ssl.rb: Default to TLSv1.2 and drop TLS v1  
Patch provided by @claudijd [Fixes GH-873] [Feature #11524]:  
<https://github.com/ruby/ruby/pull/873>

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@52082 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

##### Revision 4b395bb4 - 10/08/2015 05:26 AM - zzak (zzak \_)

- ext/openssl/lib/openssl/ssl.rb: Default to TLSv1.2 and drop TLS v1  
Patch provided by @claudijd [Fixes GH-873] [Feature #11524]:  
<https://github.com/ruby/ruby/pull/873>

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@52082 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

##### Revision e2d79c46c8eed683e95ec2b22b179980fe7b97fc - 10/09/2015 05:20 AM - sorah (Sorah Fukumori)

- ext/openssl/lib/openssl/ssl.rb: Revert r52082 because it was dropping TLS v1.1 support too. Supporting only TLS v1.2 is too early, because many popular websites still don't support it.

For instance, Servers where aws-sdk connects to still don't support TLS v1.2 and it became broken.

We should consider more carefully about this.

[Fix GH-873] [Feature #11524]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@52089 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

##### Revision e2d79c46 - 10/09/2015 05:20 AM - sorah (Sorah Fukumori)

- ext/openssl/lib/openssl/ssl.rb: Revert r52082 because it was dropping TLS v1.1 support too. Supporting only TLS v1.2 is too early, because many popular websites still don't support it.

For instance, Servers where aws-sdk connects to still don't support TLS v1.2 and it became broken.

We should consider more carefully about this.

[Fix GH-873] [Feature #11524]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@52089 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

## History

---

### #1 - 09/13/2015 03:13 AM - zzak (zzak \_)

- Assignee changed from *hsbt (Hiroshi SHIBATA)* to *7150*

### #2 - 10/08/2015 05:27 AM - zzak (zzak \_)

- Status changed from *Open* to *Closed*

Applied in changeset r52082.

---

- ext/openssl/lib/openssl/ssl.rb: Default to TLSv1.2 and drop TLS v1  
Patch provided by @claudijd [Fixes GH-873] [Feature [#11524](#)]:  
<https://github.com/ruby/ruby/pull/873>