Ruby master - Feature #17173

open-uri で ciphers を設定したい

09/16/2020 04:55 AM - znz (Kazuhiro NISHIYAMA)

Status:	Open
Priority:	Normal
Assignee:	akr (Akira Tanaka)
Target version:	

Description

Debian GNU/Linux 10 (buster) の OpenSSL 1.1.1d の環境だと https://www.famitsu.com で dh key too small になってつながらないのですが、 ciphers に DEFAULT:!DH を設定するとつながるので、 open-uri 経由でも ciphers を設定したいです。

curl での確認:

```
% curl --head https://www.famitsu.com/
curl: (35) error:141A318A:SSL routines:tls_process_ske_dhe:dh key too small
zsh: exit 35    curl --head https://www.famitsu.com/
% curl --ciphers 'DEFAULT:!DH' --head https://www.famitsu.com/
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Wed, 16 Sep 2020 04:48:25 GMT
Content-Type: text/html
Connection: keep-alive
Vary: Accept-Encoding
Accept-Ranges: bytes
Vary: Accept-Encoding
Strict-Transport-Security: max-age=60
```

ruby での確認:

```
% ruby -r open-uri -e 'open("https://www.famitsu.com/")'
Traceback (most recent call last):
        13: from -e:1:in `<main>'
        12: from /usr/lib/ruby/2.5.0/open-uri.rb:35:in `open'
        11: from /usr/lib/ruby/2.5.0/open-uri.rb:735:in `open'
        10: from /usr/lib/ruby/2.5.0/open-uri.rb:165:in `open_uri'
         9: from /usr/lib/ruby/2.5.0/open-uri.rb:224:in `open_loop'
         8: from /usr/lib/ruby/2.5.0/open-uri.rb:224:in `catch'
         7: from /usr/lib/ruby/2.5.0/open-uri.rb:226:in `block in open_loop'
         6: from /usr/lib/ruby/2.5.0/open-uri.rb:755:in `buffer_open'
         5: from /usr/lib/ruby/2.5.0/open-uri.rb:337:in `open_http'
         4: from /usr/lib/ruby/2.5.0/net/http.rb:909:in `start'
         3: from /usr/lib/ruby/2.5.0/net/http.rb:920:in `do_start'
         2: from /usr/lib/ruby/2.5.0/net/http.rb:985:in `connect'
         1: from /usr/lib/ruby/2.5.0/net/protocol.rb:44:in `ssl_socket_connect'
/usr/lib/ruby/2.5.0/net/protocol.rb:44:in `connect_nonblock': SSL_connect returned=1 errno=0 state
=error: dh key too small (OpenSSL::SSL::SSLError)
zsh: exit 1     ruby -r open-uri -e 'open("https://www.famitsu.com/")'
% ruby -r net/http -e 'http=Net::HTTP.new("www.famitsu.com", 443); http.use_ssl=true; http.ciphers
="DEFAULT:!DH"; p http.get("/")'
#<Net::HTTPOK 200 OK readbody=true>
```

https://www.ssllabs.com/ssltest/analyze.html?d=www.famitsu.com によると Cipher Suites は

```
# TLS 1.2 (suites in server-preferred order)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)   DH 1024 bits   FS   WEAK   256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)   DH 1024 bits   FS   WEAK   128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)   DH 1024 bits   FS   WEAK   256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)   DH 1024 bits   FS   WEAK   128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)   WEAK   256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)   WEAK   128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)   WEAK   256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)   WEAK   128
```

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)   ECDH secp384r1 (eq. 7680 bits RSA)   FS    256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)   ECDH secp384r1 (eq. 7680 bits RSA)   FS    128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)   ECDH secp384r1 (eq. 7680 bits RSA)   FS   WEAK 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)   ECDH secp384r1 (eq. 7680 bits RSA)   FS   WEAK 128
```

となっていて、Handshake Simulationでは

```
Chrome 80 / Win 10  R   RSA 2048 (SHA256)   TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384  No FS
Firefox 73 / Win 10  R  RSA 2048 (SHA256)   TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   ECDH secp256r1  FS
OpenSSL 1.1.1c  R   RSA 2048 (SHA256)   TLS 1.2 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384   DH 1024  FS
```

のようになっていて、TLS_DHE_RSA_WITH_AES_256_GCM_SHA384が選ばれてDH 1024 bitを拒否するクライアントからは繋らない設定になっているサーバーがあるようです。(dh key too smallでweb検索すると同様の設定のサーバーは他にもあるようです。)

History

#1 - 09/25/2020 09:17 AM - akr (Akira Tanaka)

net/httpのciphersを設定するssl_ciphersキーワード引数をopen-uriに加えるのはあり得ると思います。