Redmine - Defect #31755
Couldn't download Redmine by curl in Debian buster

2019-07-19 10:43 - Seiei Miyagi

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	

Description

In debian buster, failed.

```
% docker run --rm -it debian:buster
root@26737ff8e626:/# apt update && apt install curl -y
root@26737ff8e626:/# curl -I https://redmine.org
curl: (35) error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol
root@26737ff8e626:/# curl -vI https://redmine.org
* Expire in 0 ms for 6 (transfer 0x55ec91433dd0)
* Expire in 1 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 1 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 2 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 2 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 2 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 0 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 4 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 1 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 1 ms for 1 (transfer 0x55ec91433dd0)
* Expire in 2 ms for 1 (transfer 0x55ec91433dd0)
*   Trying 46.4.36.71...
* TCP_NODELAY set
* Expire in 200 ms for 4 (transfer 0x55ec91433dd0)
* Connected to redmine.org (46.4.36.71) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: none
  CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (OUT), TLS alert, protocol version (582):
* error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol
* Closing connection 0
curl: (35) error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol
```

```
root@26737ff8e626:/# curl -V
curl 7.64.0 (x86_64-pc-linux-gnu) libcurl/7.64.0 OpenSSL/1.1.1c zlib/1.2.11 libidn2/2.0.5 libpsl/0.20.2 (+libidn2/2.0.5)
libssh2/1.8.0 nghttp2/1.36.0 librtmp/2.3
Release-Date: 2019-02-06
Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtmp rtsp scp sftp smb smbs smtp smtps telnet
tftp
Features: AsynchDNS IDN IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB SSL libz TLS-SRP HTTP2
UnixSockets HTTPS-proxy PSL
```

In debian stretch, success.

```
% docker run --rm -it debian:stretch
root@b18b86448650:/# apt update && apt install curl -y
root@b18b86448650:/# curl -vI https://redmine.org
* Rebuilt URL to: https://redmine.org/
*   Trying 46.4.36.71...
* TCP_NODELAY set
* Connected to redmine.org (46.4.36.71) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Client hello (1):
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS change cipher, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.0 / DHE-RSA-AES256-SHA
* ALPN, server did not agree to a protocol
* Server certificate:
*  subject: OU=Domain Control Validated; OU=Gandi Standard SSL; CN=redmine.org
*  start date: Nov  5 00:00:00 2017 GMT
*  expire date: Nov 11 23:59:59 2019 GMT
*  subjectAltName: host "redmine.org" matched cert's "redmine.org"
*  issuer: C=FR; ST=Paris; L=Paris; O=Gandi; CN=Gandi Standard SSL CA 2
*  SSL certificate verify ok.
> HEAD / HTTP/1.1
> Host: redmine.org
> User-Agent: curl/7.52.1
> Accept: */*
>
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Date: Fri, 19 Jul 2019 08:24:36 GMT
```

Date: Fri, 19 Jul 2019 08:24:36 GMT
< Server: Apache
Server: Apache
< X-UA-Compatible: IE=Edge,chrome=1
X-UA-Compatible: IE=Edge,chrome=1
< ETag: "d862fcd307564c280b55a91f5ccabd02"
ETag: "d862fcd307564c280b55a91f5ccabd02"
< Cache-Control: max-age=0, private, must-revalidate
Cache-Control: max-age=0, private, must-revalidate
< X-Request-Id: d6b094973b691b257f46884fab5fad97
X-Request-Id: d6b094973b691b257f46884fab5fad97
< X-Runtime: 0.090759
X-Runtime: 0.090759
< X-Rack-Cache: miss
X-Rack-Cache: miss
< Set-Cookie:
_redmine_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFRkkiJTdkOTg2OGVmZjg0ZTYzNDE2YzViOWQzNDE0Y2VkYzQ2BjsAVEkiEF9jc
AVEkiEF9jc3JmX3Rva2VuBjsARkkiMUhaNVM1ekxQNUdxYkdta3BOUnNEajgzMUcwMG0xcnZjeGpnOHdDUSszaHM9BjsARg%3D%3D--
%3D%3D--04a0e08b3bceb4b6605986f4fefe603512be714d; path=/; HttpOnly
Set-Cookie:
_redmine_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFRkkiJTdkOTg2OGVmZjg0ZTYzNDE2YzViOWQzNDE0Y2VkYzQ2BjsAVEkiEF9jc
AVEkiEF9jc3JmX3Rva2VuBjsARkkiMUhaNVM1ekxQNUdxYkdta3BOUnNEajgzMUcwMG0xcnZjeGpnOHdDUSszaHM9BjsARg%3D%3D--
%3D%3D--04a0e08b3bceb4b6605986f4fefe603512be714d; path=/; HttpOnly
< Vary: Accept-Encoding
Vary: Accept-Encoding
< Content-Type: text/html; charset=utf-8
Content-Type: text/html; charset=utf-8

<
* Curl_http_done: called premature == 0
* Connection #0 to host redmine.org left intact
root@b18b86448650:/# curl -V
curl 7.52.1 (x86_64-pc-linux-gnu) libcurl/7.52.1 OpenSSL/1.0.2s zlib/1.2.8 libidn2/0.16 libpsl/0.17.0 (+libidn2/0.16) libssh2/1.7.0
nghttp2/1.18.1 librtmp/2.3
Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtmp rtsp scp sftp smb smbs smtp smtps telnet
tftp
Features: AsynchDNS IDN IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB SSL libz TLS-SRP HTTP2
UnixSockets HTTPS-proxy PSL

History

#1 - 2019-07-19 10:48 - Seiei Miyagi

- File Screenshot 2019-07-19 17.26.24.png added

https://redmine.org looks using TLSv1.0, maybe debian buster doesn't support TLS 1.0.

The Security tab of Chrome developer tools shows following message.

> *Connection - obsolete connection settings*
>
> *The connection to this site is encrypted and authenticated using TLS 1.0, RSA, and AES_128_CBC with HMAC-SHA1.*

> *- TLS 1.0 is obsolete. Enable TLS 1.2 or later.*
> *- RSA key exchange is obsolete. Enable an ECDHE-based cipher suite.*
> *- AES_128_CBC is obsolete. Enable an AES-GCM-based cipher suite.*

#2 - 2019-07-22 09:40 - Seiei Miyagi

FYI

> *Probably the cause is explained here:*
> *https://medium.com/@andrewhowdencom/mysterious-ssl-tls-network-connection-failures-in-debian-buster-52c29a661cb3*

https://github.com/agileware-jp/redmine-plugin-orb/pull/13#issuecomment-513328526

Files

Screenshot 2019-07-19 17.26.24.png	523 KB	2019-07-19	Seiei Miyagi