Redmine - Defect #35979
SSL Bad certificate

2021-10-11 14:53 - sacha b

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Website (redmine.org)	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	

Description

Salut,

when you use:
wget -d https://www.redmine.org/releases/redmine-4.2.3.tar.gz <= KO
curl https://www.redmine.org/releases/redmine-4.2.3.tar.gz --output redmine-4.2.3.tar.gz <= OK
enyo|14:28:52|:/home/sacha# wget -4d https://www.redmine.org/releases/redmine-4.2.3.tar.gzDEBUG output created by Wget 1.21 on linux-gnu.Reading HSTS entries from /root/.wget-hstsURI encoding = « UTF-8 »Converted file name 'redmine-4.2.3.tar.gz' (UTF-8) -> 'redmine-4.2.3.tar.gz' (UTF-8)--2021-10-11 14:30:02-- https://www.redmine.org/releases/redmine-4.2.3.tar.gzCertificates loaded: 121Résolution de www.redmine.org (www.redmine.org)… 46.4.101.126Caching www.redmine.org => 46.4.101.126Connexion à www.redmine.org (www.redmine.org)|46.4.101.126|:443… connecté.Created socket 3.Releasing 0x0000564a662eebe0 (new refcount 1).Erreur : le certificat de « www.redmine.org » n'est pas de confiance.Erreur : le certificat de « www.redmine.org » n'est pas d'un émetteur connu.Erreur : le certificat de « www.redmine.org » a expiré.
You an Usertrust chain expired since 2020 and the Gandi intermediate since last spring.

Kind regards

History

#1 - 2021-10-11 21:44 - Holger Just

The provided intermediate certificate is the "Gandi Standard SSL CA 2" certificate. Its valid until 2024-09-11, i.e. about three years from now.

The provided chain does indeed send additional (expired) certificates. However, those should generally be ignored by your TLS client library as it can use its own trust store to validate the chain against its own (local) version of the "USERTrust RSA Certification Authority" certificate. The one shipped with Chrome and Firefox is valid until 2038-01-18. Here, the clients are able to verify a complete trusted certificate chain.

With that being said, some older TLS client libraries (most prominently OpenSSL < 1.1.1) do not attempt to try to validate alternate chains and abort the TLS connection. To fix this, you could (and should) try to update the TLS client library used by your wget.

#2 - 2022-04-11 10:15 - Jan Niggemann (redmine.org team member)

- Status changed from New to Closed

- Resolution set to Invalid

See Holgers comment, closing this one.