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.gz DEBUG output created by Wget 1.21 on linux-gnu. Reading HSTS entries from /root/.wget-hsts URI 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.gz Certificates loaded: 121 Résolution de www.redmine.org (www.redmine.org)… 46.4.101.126 Caching www.redmine.org => 46.4.101.126 Connexion 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.

#3 - 2022-08-02 13:50 - Vincent Caron

It's true that the HTTPS client should pick the valid issuer and ignore the invalid/exired one (`wget` being known for this long-standing bug, even in 1.21 from 2021/01), but still I think www.redmine.org's HTTPs server should not send intermediate CA certs which have expired a long time ago :

https://www.ssllabs.com/ssltest/analyze.html?d=www.redmine.org says those 4 CAs are sent along 'www.redmine.org' cert :

- Gandi Standard SSL CA 2 : OK (expires 2024/09/11)
- USERTrust RSA Certification Authority : NOK (expired 2020/05/30, +2 years ago)
- AddTrust External CA Root : NOK (expired 2020/05/30, +2 years ago)
- UTN - DATACorp SGC : NOK (expired 2019/06/24, +3 years ago)

That's not a good admin pratice to bundle those 3 invalid CAs and I think a server-side fix would also help. The HTTPS server should only bundle the "Gandi Standard SSL CA" cert.