Redmine - Defect #33544
One of the SSL Certificates of redmine.org seems to be expired

2020-06-03 08:24 - Kevin Fischer

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

Description

It's not possible to use curl with redmine.org anymore (using it in our CI so a lot of jobs are now suddenly failing)

```
> curl https://redmine.org/
curl: (60) SSL certificate problem: certificate has expired
More details here: https://curl.haxx.se/docs/sslcerts.html

curl performs SSL certificate verification by default, using a "bundle"
 of Certificate Authority (CA) public keys (CA certs). If the default
 bundle file isn't adequate, you can specify an alternate file
 using the --cacert option.
If this HTTPS server uses a certificate signed by a CA represented in
 the bundle, the certificate verification probably failed due to a
 problem with the certificate (it might be expired, or the name might
 not match the domain name in the URL).
If you'd like to turn off curl's verification of the certificate, use
 the -k (or --insecure) option.
HTTPS-proxy has similar options --proxy-cacert and --proxy-insecure.
```

https://www.sslshopper.com/ssl-checker.html#hostname=redmine.org

History

#1 - 2020-06-09 23:26 - Holger Just

This is caused by the expiration of the "AddTrust External CA Root" intermediate certificate. For browsers (and most other current clients), this is not an issue since they are able to build a valid certificate chains without this expired intermediate certificate.

Some SSL libraries, including Openssl 1.0.x and GnuTLS strictly follow the certificate chains offered by the sever and don't try to build an alternate chain of trust of some part fails (e.g. due to expiration as we have seen here). OpenSSL 1.1 and most browsers do the correct thing here.

Still, this issue is simple to fix: just remove the top-most intermediate certificate (i.e. the from the "AddTrust External CA Root" certificate) from the list of intermediate certificates ion the server. After a reload, even those older clients should be happy again.

More details about the issue are described on https://www.agwa.name/blog/post/fixing_the_addtrust_root_expiration

#2 - 2020-06-25 11:49 - Daniel Petat

The problem also affects the sourcecode Repository

```
c:\Development\_ThirdParty\Redmine>svn checkout https://svn.redmine.org/redmine/trunk
Error validating server certificate for 'https://svn.redmine.org:443':
 - The certificate is not issued by a trusted authority. Use the
   fingerprint to validate the certificate manually!
 - The certificate has expired.
Certificate information:
 - Hostname: svn.redmine.org
 - Valid: from Jan  8 00:00:00 2020 GMT until Jan  8 23:59:59 2022 GMT
 - Issuer: Gandi Standard SSL CA 2, Gandi, Paris, Paris, FR
 - Fingerprint: 43:82:9E:5D:66:7E:A1:75:C5:ED:66:9A:BF:33:F3:59:6A:E5:AC:93
```

using TortoiseSVN version 1.14.0, including OpenSSL 1.1.1g 21 Apr 2020, which should have this problem resolved?