QGIS Application - Feature request #15617
QGIS/Qt does not trigger auto-import of Windows root Certificate Authorities

2016-09-26 04:50 AM - Luigi Pirelli

Status:	Open		
Priority:	Normal		
Assignee:	Larry Shaffer		
Category:	Authentication system		
Pull Request or Patch supplied:	No	**Resolution:**	
Easy fix?:	No	**Copied to github as #:**	23540

Description

The following steps demonstrate that QGIS/Qt is not able to trigger auto-importing of trusted root CAs by the Windows OS. Since OpenSSL is used and not the appropriate Win Crypto API calls
To verify, the procedure is:

1. Open the Windows certificate manager application (certmgr.msc) and *remove* the "AddTrust External CA Root" certificate if it exists (Note: removal is not detrimental to the Win OS, as this CA is not generally installed with a fresh copy of the OS, and it can readily be re-imported)
2. Leave the certificate manager open
3. Open QGIS and add the following plugin repo https://qgis.boundlessgeo.com/plugins.xml?qgis=2.14 (this is for testing only, because the endpoint is known to exihibt the issue; other general, non-plugin-repo SSL endpoints may as well)
4. Reload plugin repos
5. Confirm loading the new repo URL generates an SSL Error dialog indicating a missing root CA. Because boundlessgeo.com's SSL certificate is signed by "AddTrust External CA Root" the error should be produced. (**Do not ignore or save an override configuration for this error**, but abort the error to avoid the connection from being cached)
6. Open a Web browser based upon native APIs for interacting with the Win keystore, e.g. Chrome , Edge or Internet Explorer (not Firefox, since it has its own internal keystore)
7. Go to the link https://qgis.boundlessgeo.com/plugins.xml?qgis=2.14 (automatically the Windows OS should install the "AddTrust External CA Root" certificate, in the background, since it is from Comodo, a partner of the Trusted Root Certificate program hosted by Microsoft: http://social.technet.microsoft.com/wiki/contents/articles/31634.microsoft-trusted-root-certificate-program-participants-v-2016-april.aspx)
8. Refresh the certificate manager list of CAs to verify that "AddTrust External CA Root" has been added automatically (see screen shot attachment for Win 10)
9. WITHOUT closing QGIS, repeat reloading of the plugin repos
10. Confirm the same SSL error, and clicking on button "Connection trusted CAs" does not list the "AddTrust External CA Root" cert. Qt is not synched with current status/changes of the Win OS keystore. (NOTE: this is currently expected behavior, as the trusted root CA is not continuously updated by QgsAuthManager, though it should be updated in this circumstance)
11. Relaunch QGIS
12. Verify the plugin repo connection now produces **no SSL error**, as the Win OS CA trusted root list has be synchronized and cached on QGIS startup and the "AddTrust External CA Root" cert is now available.

This shows the following issues that need addressed:

- QgsAuthManager needs to update its cache whenever the Win OS keystore's trusted root CAs change (Qt may already do this, but QgsAuthManager only caches the keystore query of the root CAs on QGIS startup, or when one is added via the GUI in QGIS's Certificate Manager)
- Connecting to an endpoint in QGIS/Qt that *should* trigger the Win OS to auto-import the needed CA does not. This would happen if using a normal Web browser built upon Win Crypto API calls.

Proposed solutions:

- For QgsAuthManager, do quick comparison of Qt-provided root CAs against those that are cached, inside of QgsNetworkAccessManager. Update QgsAuthManager's cache as needed.
- When SSL error dialog is presented on Windows, and the error(s) contains "missing root CA", add a notification in the dialog that

simply explains the issue and offers the user a link or button to open the same URL in the default browser, which would possibly auto-import the root CA (but not if the browser is Firefox). This may be an easier fix than trying to programmatically call the Win Crypto API to possibly auto-update the missing root CA and reattempt the connection.

History

#1 - 2016-09-26 07:22 AM - Giovanni Manghi

- Subject changed from QGIS/QT Does not update list of Trusted CAs => need qgi srestart to QGIS/QT Does not update list of Trusted CAs => need QGIS srestart

#2 - 2016-09-26 07:26 AM - Giovanni Manghi

- Subject changed from QGIS/QT Does not update list of Trusted CAs => need QGIS srestart to QGIS/QT Does not update list of Trusted CAs => need QGIS restart

#3 - 2016-09-26 07:36 AM - Jürgen Fischer

- Project changed from QGIS Redmine (QGIS bug tracker) to QGIS Application

#4 - 2016-09-26 08:14 AM - Giovanni Manghi

- Assignee set to Larry Shaffer

#5 - 2016-09-26 08:37 AM - Larry Shaffer

- Target version set to Version 2.18

- Category set to Authentication system

#6 - 2016-09-26 09:19 AM - Larry Shaffer

- Subject changed from QGIS/QT Does not update list of Trusted CAs => need QGIS restart to QGIS/Qt does not trigger auto-import of Windows root Certificate Authorities

#7 - 2016-09-26 09:22 AM - Larry Shaffer

- File qgis-trusted-cas-cached.png added

#8 - 2016-09-26 09:38 AM - Larry Shaffer

Regarding the qgis-trusted-cas-cached.png attachment. The left part of the image shows the *default trusted root CAs* for a fresh install of Windows 10, *plus* the "AddTrust External CA Root" certificate that was added automatically by the Win OS via its hosted Trusted Root Certificate program.

#9 - 2016-10-10 01:38 AM - Luigi Pirelli

during dev I found a possible bug reported in #15687

#10 - 2016-10-17 02:45 AM - Luigi Pirelli

I didn't find any solution to #15687 => the only way to reload ssl CA cache without waiting some minutes for the update is to re-start qgis!

#11 - 2016-10-17 02:54 AM - Luigi Pirelli

I'll prepare a PR from the following branch:

https://github.com/boundlessgeo/qgis/tree/CAs_import_via_keystore the fix is applicable only on Windows. No CA problems found on linux and mac.

#12 - 2016-10-17 02:58 AM - Luigi Pirelli

just waiting to have a UX review before to create the PR

#13 - 2016-10-17 06:25 AM - Luigi Pirelli

a screencast to show hos the interface works
https://youtu.be/pN30XE7r7_k

#14 - 2016-10-19 04:21 AM - Luigi Pirelli

created two PR

for 2.14: https://github.com/qgis/QGIS/pull/3640
for 2.18: https://github.com/qgis/QGIS/pull/3671

#15 - 2016-10-19 04:33 AM - Luigi Pirelli

fix only for 2.14 and release-2_18 because probably the issue is not present in qgis3 due the different ssl infrastructure offered by qt5

#16 - 2017-05-01 12:46 AM - Giovanni Manghi

- Easy fix? set to No

Files

qgis-trusted-cas-cached.png	448 KB	2016-09-26	Larry Shaffer