QGIS Application - Feature request #11473
Use TLS v1.2 instead of SSL v3

2014-10-22 11:41 PM - guillaume -

Status:	Closed		
Priority:	High		
Assignee:	Jürgen Fischer		
Category:	Web Services clients/WMS		
Pull Request or Patch supplied:	No	**Resolution:**	
Easy fix?:	No	**Copied to github as #:**	19743

Description

For HTTPS connections, QGIS uses SSL V3 which is old and weak (a major failure has been discovered recently, see https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-poodle-sslv3-vulnerability). This weakness and the Poodle vulnerability are going to make most servers stop using SSL v3 as recommended. Hence, QGIS won't be able to establish a connection to them.
QGIS should move to TLS 1.2 quickly.

Best regards

Related issues:

Related to QGIS Application - Bug report # 11499: Style manager fails to load...	**Closed**	**2014-10-25**
Related to QGIS Application - Bug report # 11479: Direct printing only prints...	**Closed**	**2014-10-23**
Related to QGIS Application - Bug report # 11145: Large format export/printin...	**Closed**	**2014-09-05**

History

#1 - 2014-10-23 06:46 AM - guillaume -

Sorry for the noise, QGIS is already designed with TLS 1.2

#2 - 2014-11-19 07:42 AM - Neil Benny

TLS 1.2 on QGIS only seems to be in place for the 64 bit version (32 bit doesn't work) and I'm having some problems following a recent security upgrade to our WMS which shut down SSL v3.

Am I missing something obvious – does it need turned on somewhere?

#3 - 2014-11-28 03:32 AM - Matt Debont

We recently had to shut down SSL V3 on our WMS and this issue started cropping up and it does appear to be a 32 bit specific problem which while not a problem for myself, it is hitting a section of our users (can't / won't upgrade to a 64 bit OS).

Would be great to know if anyone has figured out how to get TLS 1.2 to work on the 32 bit app however, or if I am simply missing something obvious.

#4 - 2014-11-28 05:47 AM - Jürgen Fischer

Matt Debont wrote:

> *We recently had to shut down SSL V3 on our WMS and this issue started cropping up and it does appear to be a 32 bit specific problem which while not a problem for myself, it is hitting a section of our users (can't / won't upgrade to a 64 bit OS).*

> *Would be great to know if anyone has figured out how to get TLS 1.2 to work on the 32 bit app however, or if I am simply missing something obvious.*

Probably not, because it takes a newer Qt version - and a rebuild of everything depending on it.

#5 - 2015-01-16 10:24 AM - Jürgen Fischer

- Assignee set to Jürgen Fischer

#6 - 2015-01-18 07:22 AM - David Lee

Please can you explain whether this means that this problem will be fixed and, if so, the expected timescale?

The lack of TLS support in the 32 bit version of QGIS is having a major impact upon ecologists in the UK since it blocks access to the WMS server of the official UK national biological records centre (National Biodiversity Network Gateway) for users unable to use the 64 bit application.

Since QGIS is said to have been designed with TLS 1.2 in place, the lack of TLS functionality in the 32 bit version would appear to be a serious bug rather than merely a "feature request".

#7 - 2015-01-21 04:16 AM - Jürgen Fischer

- Status changed from Open to Closed

Qt in OSGeo4W 32bit was updated to 4.8.6

#8 - 2015-01-21 06:55 AM - David Lee

It would have been more helpful if you had explained that Qt has only been updated to 4.8.6 in the Network Installer download of 32bit QGIS - "For Advanced Users"!

The Standalone version - which will be downloaded by the vast majority of users - still installs QT 4.7.1.

#9 - 2015-01-21 07:16 AM - Giovanni Manghi

David Lee wrote:

> *It would have been more helpful if you had explained that Qt has only been updated to 4.8.6 in the Network Installer download of 32bit QGIS - "For Advanced Users"!*
>
> *The Standalone version - which will be downloaded by the vast majority of users - still installs QT 4.7.1.*

FYI the standalone installers are derived/created using the packages in the osgeo4w installer, so it is just a matter to wait for the next (standalone) build.

#10 - 2015-01-21 07:45 AM - Jürgen Fischer

David Lee wrote:

>

> *It would have been more helpful if you had explained that Qt has only been updated to 4.8.6 in the Network Installer download of 32bit QGIS - "For Advanced Users"!*
> *The Standalone version - which will be downloaded by the vast majority of users - still installs QT 4.7.1.*

Sorry for the confusion, I thought "OSGeo4W 32bit" was explicit enough.

#11 - 2015-01-21 09:13 AM - David Lee

Not really. OSGeo4W is installed whether you use the QGIS standalone installer or the network installer, so I initially assumed that they would both deliver the same updated version.

The remaining question is - when will the standalone installer be rebuilt and how can we know when it has happened? It's rather inconvenient to have to download everything again for each machine on which you want to install QGIS, so a single download of the standalone package is much more efficient.

#12 - 2015-01-22 08:25 AM - Giovanni Manghi

David Lee wrote:

> *Not really. OSGeo4W is installed whether you use the QGIS standalone installer or the network installer, so I initially assumed that they would both deliver the same updated version.*

no, it is not like that. If you install qgis standalone then osgeo4w is not installed. But QGIS standalone is made of the very same (binary) packages that are available in osgeo4w. In fact in the qgis source code you even have a script that allows you to build the standalone installer. The script takes the packages from the osgeo4w repository and "assemble" them into the standalone installer.

#13 - 2015-01-22 09:37 AM - David Lee

Clearly I'm just confused!
I naively assumed that the appearance of an OSGeo4W command shell icon on my desktop meant that the Standalone installer had installed OSGeo4W!

Can anyone answer the question "When will the Standalone installer be rebuilt to include the latest version of QT"?

Alternatively, Giovanni's reply suggests that I should be able to create a standalone installer myself from the OSGeo4W Advanced installer that I could then share with our other 32bit users. Is that the case and if so how do I do it?

Sorry if I'm being particularly dim!

#14 - 2015-01-22 10:23 AM - Giovanni Manghi

David Lee wrote:

> *Clearly I'm just confused!*
> *I naively assumed that the appearance of an OSGeo4W command shell icon on my desktop meant that the Standalone installer had installed OSGeo4W!*

nope, it just installs the same command line shell, among the other things.

> *Can anyone answer the question "When will the Standalone installer be rebuilt to include the latest version of QT"?*

I believe that are rebuilt when necessary, for example when a serious bug is backported, or something like that.

Right now the worst case scenario is that you will have a new standalone installers in one month, as qgis 2.8 is due in more or less 30 days.

> *Alternatively, Giovanni's reply suggests that I should be able to create a standalone installer myself from the OSGeo4W Advanced installer that I could then share with our other 32bit users. Is that the case and if so how do I do it?*

https://github.com/qgis/QGIS/blob/master/ms-windows/osgeo4w/creatensis.pl