Quassel IRC - Feature #1323

It doesn't seem to be possible to disable SSLv3.

11/04/2014 08:24 PM - ddenis

Status:	Resolved	**Start date:**	11/04/2014
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
OS:	Any		

Description

SSLv3 is considered harmful (see CVE-2014-3566 aka POODLE) but it seems to be used by default for QuasselCore / Client.

As far as I understand the default ssl protocol for QSslSocket is SSLv3 and TLSv1.0 (that is covered by QSsl::SecureProtocol enum value which is the default). There is a fix in Qt to not include SSLv3 in QSsl::SecureProtocols however it hasn't been released yet (and seems to be in upcoming 5.4 only - https://qt.gitorious.org/qt/qtbase/commit/3fd2d9eff8c1f948306ee5fbfe364ccded1c4b84).

It would be great if it is possible to enforce TLS-only connections with Quassel.

Related issues:

Related to Quassel IRC - Bug #1728: Core launched with --require-ssl flag, bu...	**Resolved**	**06/16/2021**

History

#1 - 06/16/2021 08:57 PM - phuzion

- Related to Bug #1728: Core launched with --require-ssl flag, but no certificate to load, will accept plaintext connections added

#2 - 06/16/2021 08:58 PM - phuzion

Hi there. I'm going through the backlog of bugs in the queue and handling ones I think I can help out with.

I've just done a test with openssl s_client, on quasselcore built from source, and my build is only supporting TLS 1.0, 1.1 and 1.2. No SSLv3 is supported. I also tested the Fedora-packaged Quasselcore (0.13.1) and it also does not support SSLv3. I do not believe that any modern builds of Quassel support SSLv3 anymore.

In testing this bug, I also discovered #1728, which currently has a PR submitted to fix. Once that is merged, this bug should be good to close.

#3 - 06/18/2021 03:57 PM - phuzion

- Status changed from New to Resolved

With #1728 resolved, I'm happy to say this bug is fully resolved. Thanks for the report!