

Quassel IRC - Bug #1491

Quassel client: Error while setting the maximum protocol version

09/11/2018 08:15 AM - xypron

Status:	Closed	Start date:	09/11/2018
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:	Some future release	OS:	Any
Version:	0.12.4		

Description

My Debian Buster installation of the Quassel client (version 0.12.5) fails to connect with the message "Error while setting the maximum protocol version". I verified with Wireshark that my Linux client is actually communicating to the server on port 4242.

This seems to relate to code in
qt5/qtbase/src/network/ssl/qsslcontext_openssl11.cpp.html.

I have no problem to connect to my server with the Android client.

The error did not occur before version 5.11.1+dfsg-7 of qtbase was released to Debian testing on Sept. 10, 2018.

The relevant code in qtbase was changed with
e3cea2a7b9f8 ("QSslSocket (OpenSSL 1.1) - respect requested protocol version").

This is the protocol information provided by openssl:

```
$ openssl s_client connect myserver.domain:4242 -proxit
CONNECTED
write:errno=0
-
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 176 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
Protocol : TLSv1.2
Cipher : 0000
Session-ID:
Session-ID-ctx:
Master-Key:
PSK identity: None
PSK identity hint: None
SRP username: None
Start Time: 1536645791
Timeout : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: no
---
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 176 bytes
```

Verification: OK

New, (NONE), Cipher is (NONE)

Secure Renegotiation IS NOT supported

Compression: NONE

Expansion: NONE

No ALPN negotiated

SSL-Session:

Protocol : TLSv1.2

Cipher : 0000

Session-ID:

Session-ID-ctx:

Master-Key:

PSK identity: None

PSK identity hint: None

SRP username: None

Start Time: 1536645791

Timeout : 7200 (sec)

Verify return code: 0 (ok)

Extended master secret: no

History

#1 - 09/14/2018 02:42 AM - genius3000

- *Status changed from New to Closed*

Closing as this ended up being a Qt bug, which appears to have been fixed recently.

Reference bug report: <https://www.mail-archive.com/debian-qt-kde@lists.debian.org/msg83420.html>

Reference commit: <https://code.qt.io/cgi/qt/qtbase.git/commit/?h=e3cea2a7b9f8>