Quassel IRC - Bug #1728

Core launched with --require-ssl flag, but no certificate to load, will accept plaintext connections

06/16/2021 07:30 PM - phuzion

Status:	Resolved	**Start date:**	06/16/2021
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Quassel Core	**Estimated time:**	0.00 hour
Target version:			
Version:	0.13.1	**OS:**	Any

Description

Cores launched with the "--require-ssl" flag, (introduced in https://github.com/quassel/quassel/pull/43) will reject clients that do not accept SSL.

However, if the core itself does not have an SSL certificate available to load, the core will still launch, and happily accept plaintext connections.

This is an unexpected situation.

Steps to reproduce:

1. Install Quasselcore by whatever means you wish
2. Configure Quasselcore's data directory with no quasselCert.pem file
3. Launch Quasselcore with the "--require-ssl" flag on the command line

Expected results:

Quasselcore will not launch, because the core could not find an SSL certificate.

Actual results

Quasselcore launches, and accepts plaintext client connections.

Related issues:

Related to Quassel IRC - Feature #1323: It doesn't seem to be possible to dis...	**Resolved**	**11/04/2014**

History

#1 - 06/16/2021 08:52 PM - phuzion

PR submitted to fix this.

https://github.com/quassel/quassel/pull/581

#2 - 06/16/2021 08:57 PM - phuzion

- Related to Feature #1323: It doesn't seem to be possible to disable SSLv3. added

#3 - 06/17/2021 05:34 PM - phuzion

- Priority changed from Normal to High

Per relrod on Github, this bug has been assigned CVE-2021-34825 by MITRE.

MITRE CVE link.

#4 - 06/18/2021 03:57 PM - phuzion

- Status changed from New to Resolved

PR 581 has been merged, resolving this bug.