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

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:
Resolved 11/04/2014

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

MITRE CVE link.