

## 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

<b>Status:</b>	Resolved	<b>Start date:</b>	06/16/2021
<b>Priority:</b>	High	<b>Due date:</b>	
<b>Assignee:</b>		<b>% Done:</b>	0%
<b>Category:</b>	Quassel Core	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>		<b>OS:</b>	Any
<b>Version:</b>	0.13.1		
<b>Description</b>			
<p>Cores launched with the "--require-ssl" flag, (introduced in <a href="https://github.com/quassel/quassel/pull/43">https://github.com/quassel/quassel/pull/43</a>) will reject clients that do not accept SSL.</p> <p>However, if the core itself does not have an SSL certificate available to load, the core will still launch, and happily accept plaintext connections.</p> <p>This is an unexpected situation.</p>			
<b>Steps to reproduce:</b>			
<ol style="list-style-type: none"><li>1. Install Quasselcore by whatever means you wish</li><li>2. Configure Quasselcore's data directory with no quasselCert.pem file</li><li>3. Launch Quasselcore with the "--require-ssl" flag on the command line</li></ol>			
<b>Expected results:</b>			
<p>Quasselcore will not launch, because the core could not find an SSL certificate.</p>			
<b>Actual results</b>			
<p>Quasselcore launches, and accepts plaintext client connections.</p>			
<b>Related issues:</b>			
Related to Quassel IRC - Feature #1323: It doesn't seem to be possible to dis...		<b>Resolved</b>	<b>11/04/2014</b>

## 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.