Quassel IRC - Bug #714

Quassel does not warn if SSL certificate changed on remote IRC server (not core)

06/03/2009 05:13 AM - kitterma

Status:	New	**Start date:**	06/03/2009
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Quassel Core	**Estimated time:**	0.00 hour
Target version:			
Version:	0.4.2	**OS:**	Linux

Description

One of the IRC servers I used upgraded to a new system and in the process changed their SSL certificate. All that happened is that I didn't automatically reconnect. Once I made the connection manually, it just went with no warning that the cert had changed.

While I'm not sure how important it is to do cert CA validation, I do think it's very important that if the cert for a channel changes the user is warned before reconnecting. This is important to prevent MITM attacks.

History

#1 - 06/28/2009 05:12 PM - EgS

- Priority changed from Urgent to Normal