Quassel IRC - Bug #968

Core crashes when connecting to a server with an incorrect welcome message

05/21/2010 04:01 AM - a1291762

Status:	Closed	**Start date:**	05/21/2010
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Version:	0.4.3	**OS:**	Any

Description

I ran a crappy little test IRC server (http://www.hping.org/tclircd/) and when I connected Quassel 0.6.1 to it the core crashed.

The function IrcServerHandler::handle001() is to blame.

If the params list is empty, it prints out a message and then proceeds to run code that assumes params is not empty.

I have attached a patch that stops the core crashing. Probably not the best solution but better than a crash.

History

#1 - 05/21/2010 05:32 AM - a1291762

I guess the server is just being stupid but it does at least partly seem to have something to do with the : chars that Quassel is sending. For example, Konversation registers me with NICK lramsay while Quassel sends NICK :lramsay. Because of the difference the server ends up sending the following welcome banner:

:localhost 001 :lramsay :Welcome to this IRC server lramsay

The :lramsay confuses the Quassel parsing code which is why the params list is empty. I'm not sure if Quassel should be handling this or if the IRC server should be suppressing the : in the nick...

#2 - 07/23/2010 12:56 PM - TerrorBite

I don't think Quassel is sending the NICK command correctly here. Then again, if your IRCd is accepting a nick containing invalid characters (nicks may only contain alphanumerics and the 10 characters "[\]{|}^-`_") then this is an issue with the server. As a programmer though, I think Quassel should be handling incorrect/malformed server messages gracefully instead of crashing, not least because this could be a security risk if a Quassel user connected to a malicious server (or even a regular Unreal server with the SENDRAW module and an admin who likes playing games).

#3 - 06/03/2013 06:59 PM - Anonymous

- Status changed from New to Closed

You're both right, in all respects. The ircd is wrong, quassel is arguably wrong and quassel shouldn't crash. The good news is it doesn't crash anymore, it just doesn't work with tclircd at all.

Files

stop_core_crashing.diff	864 Bytes	05/21/2010	a1291762