Quassel IRC - Bug #1399

Quassel shows STATUSMSG messages as queries

03/10/2016 09:27 AM - arathald

Status:	Resolved	**Start date:**	03/10/2016
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.12.4		
Version:	0.10.0	**OS:**	Any

Description

Some IRC servers, including Freenode, support a feature called STATUSMSG that allows a user to send a message to a channel name prefixed with a status character to limit the scope of the message. For example, a message sent to @#quassel would send a message to only users with operator status in #quassel. Most clients implement this as message channels marked in some way to make it clear it was a STATUSMSG. See https://tools.ietf.org/html/draft-brocklesby-irc-isupport-03#section-3.16 (this only mentions STATUSMSG in connection with NOTICE, but Freenode implements it with PRIVMSG as well) and http://www.irc.org/tech_docs/005.html.

Quassel, along with many other clients, are showing these messages as queries instead of channel messages. In Quassel, these messages look exactly like private queries, though they're broadcast to multiple users. I don't know precisely what the user experience on other affected clients is firsthand, though I'm led to believe they treat these messages in a way similar to Quassel.

To save you a few minutes, I did a bit of upfront investigation: On line 41 of messageevent.cpp (https://github.com/quassel/quassel/blob/master/src/common/messageevent.cpp#L41), the message event handler looks up the channel (e.g. "+#channel") in the channel list and doesn't find it. The leading '+' is then removed on lines 43-44, lines 46-47 see "#channel" as a user mask and set _target back to sender. When the call to bufferTypeByTarget() is made, the buffer is set to query, as _target is now the sender (though Network::isChannelName() wouldn't recognize "+#channel" as a valid channel, so this would still fall through to the buffer even if _target wasn't munged).

Because there's no other circumstance in which sending a message to "+#channel" is valid, because the server explicitly declares its support and wouldn't forward messages if this wasn't the intent, and because it's very easy to disambiguate a valid channel name from a prefixed user (i.e. "+#channel" and "+user" are easy to tell apart, especially if "#channel" must be a valid channel), both Network::ircChannel() and Network::isChannelName() should be safe and easy to modify to also recognize channels prefixed by a character specified in STATUSMSG.

I'd also suggest that being able to tell the difference between a STATUSMSG and a regular channel message is important (for example, if an operator starts an ops-only conversation by messaging #channel, other ops should be aware of it so they can respond in kind). One approach I saw from a client while looking into this was appending the channel name (with prefix) to the sender's name, so an ops-only STATUSMESSAGE would show up in the channel as "<User:#channel> message". As I'm unfamiliar with the standards of the Quassel project, I'm merely making this as a suggestion and leaving it up to the developers to make a decision on that.

I'm marking this as high priority because of the fairly large ability to exploit this issue with minimal effort (users were sending messages like this to hundreds of voiced users in #freenode), as well as the fact that it has been discovered and publicized on Freenode, directly in connection with Quassel, among several popular clients. As I probably don't understand the proper priority bars in this project, I wouldn't be surprised if this was inappropriate. Please feel free to reprioritize as appropriate.

Related issues:

Related to Quassel IRC - Bug #1488: Store and display a STATUSMSG correctly	**New**	**07/20/2018**

History

#1 - 05/17/2016 10:41 PM - Sputnick

- Status changed from New to Resolved

- Target version set to 0.12.4

Fixed in 0.12.4.

#2 - 07/20/2018 12:46 PM - genius3000

- Related to Bug #1488: Store and display a STATUSMSG correctly added