Quassel IRC - Bug #1118

Livelock caused by mirctohtml

11/16/2011 08:56 PM - Anonymous

Status:	New	**Start date:**	11/16/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Quassel Client	**Estimated time:**	0.00 hour
Target version:			
Version:	0.9.0	**OS:**	Any

Description

One can easily trigger a livelock in the following way:
1) Copy-pasta the stuff from http://dl.dropbox.com/u/14849789/rainbow_horseshit.txt (attached as well) into the input widget
2) Send the message and be amazed at the work of art you just sent
3) Move up to get the message again and watch your memory be devoured by quassel

It's caused by the for(;;) loop in convertMircCodesToHtml() [src/uisupport/multilineedit.cpp:556]. The problem is that for what should be the last run, 'text.indexOf(mircCode.cap(), posRight + 1)' [line 580] sets posRight to -1, as it doesn't match, resulting in posLeft being set to 0, effectively starting the loop all over.

This might be because of invalid data, wrong assumptions on the data, or something entirely else, but i'm not familiar enough with the mirc formatting to understand the loop properly. One can prevent the livelock by break'ing when posRight is -1, but this sort of messes up formatting (at least, what shows up in the chatview after sending does not equal what one gets when going back in history).

History

#1 - 12/23/2013 10:56 PM - Anonymous

- Priority changed from High to Normal

- Version changed from 0.8-pre to 0.9.0

Files

rainbow_horseshit.txt	2.29 KB	11/16/2011	Anonymous