Quassel IRC - Bug #1257

Segfault in string handling

12/20/2013 06:40 PM - bongo

Status:	Resolved	**Start date:**	12/20/2013
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Quassel Client	**Estimated time:**	0.00 hour
Target version:			
Version:	0.9-pre	**OS:**	Linux

Description

Quasselclient for linux v0.9.1 (Protocol v10) crashed when trying to view a bitlbee jabber channel with very long messages.

Reproduction:
Write a very long message to a buddy on bitlbee. To reproduce the crash, try to open the channel of that buddy.

Output on the commandline (see attached file):

```
"String too long to be styled: [long $String here]
```

Associated revisions

Revision a6c41972 - 03/01/2014 02:07 PM - Manuel Nickschas

Don't crash on very long inputs

Because our style engine uses 16 bit indexes, strings can only be styled if they're shorter than 2^16 characters. We do check for this in the style engine and refuse to style strings that are longer.

However, just returning an default-constructed StyledString() is wrong, because other places rely on there being at least one format and the plaintext be initialized. So the proper way of handling this is just using the baseFormat and the full string as plaintext instead of an empty StyledString.

Fixes #1257.

Revision 05c43ed7 - 03/01/2014 02:10 PM - Manuel Nickschas

Don't crash on very long inputs

Because our style engine uses 16 bit indexes, strings can only be styled if they're shorter than 2^16 characters. We do check for this in the style engine and refuse to style strings that are longer.

However, just returning an default-constructed StyledString() is wrong, because other places rely on there being at least one format and the plaintext be initialized. So the proper way of handling this is just using the baseFormat and the full string as plaintext instead of an empty StyledString.

Fixes #1257.

History

#1 - 12/20/2013 09:13 PM - Anonymous

- File crashlog added

- Status changed from New to Confirmed

- Priority changed from High to Normal

Easily reproducable, even by pasting the message in quassel itself (did take a while to crash the first time).

#2 - 03/01/2014 02:10 PM - Anonymous

- Status changed from Confirmed to Resolved

- % Done changed from 0 to 100

Applied in changeset quassel|commit:a6c419727506abd19f41d8de6e02de015a7aa8e5.

Files

log.log	274 KB	12/20/2013	bongo
crashlog	23.5 KB	12/20/2013	Anonymous