

Quassel IRC - Bug #1583

Regression in "Mouse wheel changes selected chat" causing crash

07/12/2020 10:47 PM - oprypin

Status:	Resolved	Start date:	07/12/2020
Priority:	Normal	Due date:	
Assignee:	digitalcircuit	% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:	0.14.0	OS:	Any
Version:	0.13.0		
Description			
<p>On latest master (not in 0.13.1 release), if "Mouse wheel changes selected chat" is enabled, scrolling over the chat list in many situations leads to a crash. One of such situations is if you just closed a chat room that was active.</p> <p>Video of repro: https://i.imgur.com/2iPiylN.mp4 quassel-scroll.webm</p> <p>https://github.com/quassel/quassel/commit/a453c963cf1872e14c83adf1d40a31821c166805 is the first bad commit</p> <p>Reproduce it:</p> <ul style="list-style-type: none">•  make printf "[ItemViews]\nMouseWheelChangesBuffer=true" >quasselclient.conf ./quassel --configdir=.• Accept all default setup• Enable Settings > Interface > Chat & Nick Lists > Mouse wheel changes selected chat ^(already ensured by the command above)• /query yourself• Right click on yourself, Hide Chat(s) Permanently• Hover over the chat list, scroll the mouse wheel crash			

Associated revisions

Revision 47b54cd3 - 10/04/2020 06:18 PM - Shane Synan

uisupport: Fix invalid model segfault from index

The Qt implementation of `QModelIndex::child(...)` automatically checks if the `QAbstractItemModel` is valid, and if not, it returns an invalid `QModelIndex`. Quassel relied upon this in several places, checking if the `QModelIndex` was valid without checking the `QAbstractItemModel` itself, which introduced crashes upon migrating away from the deprecated `QModelIndex::child(...)` function.

Specifically...

```
#if QT_DEPRECATED_SINCE(5, 8)
inline QModelIndex QModelIndex::child(int arow, int acolumn) const { return m ? m->index(arow, acolumn, *this) : QModelIndex(); }
#endif
```

To address this, check the `QModelIndex`'s model to verify it's valid wherever Quassel had previously relied upon a check to `QModelIndex::isValid()` to ensure validity. Places without a validity check aren't adjusted under the assumption it won't ever be an issue.

Follow-up to the Qt deprecation fixes in

a453c963cf1872e14c83adf1d40a31821c166805

(It's unfortunate that Qt's deprecation warning mentioned this, but only in the detailed documentation and not as clearly as expected: <https://doc.qt.io/qt-5/qmodelindex-obsolete.html>)

Special thanks to oprypin for reporting this with a detailed, reproducible test case!

Fixes #1583

History

#1 - 07/12/2020 11:16 PM - digitalcircuit

- Assignee set to digitalcircuit
- Target version set to 0.14.0

#2 - 07/17/2020 10:10 PM - digitalcircuit

This has been [fixed in a pull request, client: Fix crash on switching buffers with no buffer selected #544](#) . Once merged, this issue should automatically be closed.

If you don't mind re-compiling with the above patch, would you confirm that this issue is fixed for you as well? Optionally, if you have a GitHub account, you can comment there as well.

#3 - 07/29/2020 08:30 AM - digitalcircuit

- Status changed from New to Confirmed

#4 - 10/04/2020 06:18 PM - Anonymous

- Status changed from Confirmed to Resolved
- % Done changed from 0 to 100

Applied in changeset [quassel|47b54cd3ad35201ff2ab9ef6bfdba83fc086558d](#).

Files

quassel-scroll.webm	1.22 MB	07/12/2020	oprypin
---------------------	---------	------------	---------