Crash in QgsGeomColumnTypeThread stopping connection scan

I just got a segfault with current master (670ded3d06222811f8e0ba50b3fd5e783742044) by clicking on "stop" in the "Add PostGIS Layer" dialog, while it was scannign a database.

(gdb) bt
#0 0x00007fa6eb4ec12c in QString::QString (this=0x7fa6d98c8b40, other=...) at /usr/include/qt4/QtCore/qstring.h:725
#1 0x00007fa6eb510273 in QgsPostgresConn::connInfo (this=0x0) at /usr/src/qgis/qgis-master/src/providers/postgres/qgspostgresconn.h:308
#2 0x00007fa6eb510387 in qgsConnectionPool_ConnectionToName (c=0x0) at /usr/src/qgis/qgis-master/src/providers/postgres/qgspostgresconnpool.h:25
#3 0x00007fa6eb510c2a in QgsConnectionPool<QgsPostgresConn*, QgsPostgresConnPoolGroup>::releaseConnection (this=0x7fa6eb75ed50 <QgsPostgresConnPool::sInstance>, conn=0x0) at /usr/src/qgis/qgis-master/src/core/qgsconnectionpool.h:264
#4 0x00007fa6eb5304aa in QgsGeomColumnTypeThread::run (this=0x2337220) at /usr/src/qgis/qgis-master/src/providers/postgres/qgscolumnotypethread.cpp:115
#5 0x00007fa6eb5304aa in thread_start (arg=0x7fa6d98c9700) at pthread_create.c:312
#6 0x00007fa7801c182 in start_thread (arg=0x7fa6d98c9700) at pthread_create.c:312
#7 0x00007fa6eb5304aa in thread_start (arg=0x7fa6d98c9700) at pthread_create.c:312

It's still the QgsGeomColumnTypeThread...

Associated revisions

Revision 69cb0c4e - 2016-01-19 01:15 PM - Sandro Santilli

Fix double-release of postgresql connection on table retrieval stop

Also breaks earlier out of loop and print a different status message on "stop" (rather than "complete").

Fixes #14140
Invalid read of size 8
at 0x8355B12C: QString::QString(QString const&) (qstring.h:725)
by 0x8357F272: QgsPostgresConn::connInfo() const (qgspostgresconn.h:308)
by 0x8357F386: qgsConnectionPool_ConnectionToName(QgsPostgresConn*) (qgspostgresconnpool.h:25)
by 0x8357FC29: QgsConnectionPool<QgsPostgresConn*, QgsPostgresConnPoolGroup>::releaseConnection(QgsPostgresConn*)
(qgsconnectionpool.h:264)
by 0x8359F4A9: QgsGeomColumnTypeThread::run() (qgscolumntypeofthread.cpp:115)

#2 - 2016-01-19 03:56 AM - Sandro Santilli

Got it, ColumnTypeThread handling of "stopped" (mStop) is not thread-safe.

#3 - 2016-01-19 04:15 AM - Sandro Santilli
- Status changed from In Progress to Closed

Fixed in changeset commit:"69cb0c4ed3174946c82e32dad4af5a12275079fc".