QGIS Application - Bug report #3920
Returning address of local variable

2006-03-24 02:02 PM - Mateusz Loskot -

Status:	Closed		
Priority:	Low		
Assignee:	Gavin Macaulay -		
Category:	Vectors		
Affected QGIS version:		**Regression?:**	No
Operating System:	All	**Easy fix?:**	No
Pull Request or Patch supplied:		**Resolution:**	fixed
Crashes QGIS or corrupts data:		**Copied to github as #:**	13944

Description

In file **qgsfeature.cpp**, member function:
QString const& QgsFeature::wellKnownText() const
returns const reference to **QString** but in the body of
this function **QString::null** is returned.
null is an object of type **QString::Null**, so this return
expression returns reference to local (automatic) variable.
After program execution flow exits this function, this
reference is invalid and undefined behaviour can be
expected.

Here is small example that presents how easily the
problem explained above can cause serious crash:

```
#include <QCoreApplication>
#include <QString>
#include <iostream>

struct B
{
  QString const& foo()
  {
    return QString::null;
  }
};

int main(int argc, char *argv[])
{
  QCoreApplication app(argc, argv);
  B b;
  std::cout << b.foo().toStdString() << std::endl;
  //------------^^^^^^^^^^^^^^^^^^ ka-Boom!
  return 0;
}
```

here, **toStdString()** is called on invalid reference to not existing object, so program will crash with "Access violation" error.

IMPORTANT!
I'd recommend to make a detailed review of **all** places

where const reference to QString is returned from
function or is passed to function and QString::null is
used as a default argument value.

This example above presents only return value case but
following example may also cause problems:

```
void foo(QString const& s = QString::null)
{
  // do something with s without checking
  // if its value is QString::null
  std::cout << s.toStdString() << std::endl;
  //-----------^^^^^^^^^^^^^^^ crash
}
```

History

#1 - 2006-04-08 02:47 AM - Gavin Macaulay -

- Status changed from Open to In Progress

Resolved the given example in commit:6a7570f4 (SVN r5229). Haven't looked elsewhere for the same problem.

QString is implicitly shared, but I'm not sure if that resolves the problem for local variables returned via references (it does resolve the problem for QStrings returned via a copy).

Leaving this open as a reminder to look for and correct other instances of the same problem

#2 - 2006-04-08 02:55 AM - Gavin Macaulay -

- Resolution set to fixed

- Status changed from In Progress to Closed

The one in [[QgsFeature]] seems to be the only place where this is done, so I'm closing this ticket.

#3 - 2006-04-08 03:00 AM - Mateusz Loskot -

Yes, I dis some searching for places with similar problem and I've not found any.
So, it seems to be the only such place.

#4 - 2009-08-22 12:46 AM - Anonymous

Milestone Version 0.8 deleted