QGIS Application - Bug report #3934
std::list iterator not dereferencable bug in the QgsUniqueValueDialog

2006-03-28 03:45 PM - Mateusz Loskot -

Status:	Closed		
Priority:	Low		
Assignee:	Gary Sherman		
Category:	Map Legend		
Affected QGIS version:		**Regression?:**	No
Operating System:	Windows	**Easy fix?:**	No
Pull Request or Patch supplied:		**Resolution:**	fixed
Crashes QGIS or corrupts data:		**Copied to github as #:**	13958

Description

The Background:

The **QgsUniqueValueRenderer::classificationAttributes()** call returns a copy of the std::list<int> list:

```
std::list<int> [[QgsUniqueValueRenderer]]::classificationAttributes() const
{
  std::list<int> list;
  list.push_back(mClassificationField);
  return list;
}
```

There is no bug so far.

The constructor of **QgsUniqueValueDialog** class uses the **classificationAttributes()** in the following way:

```
std::list<int>::iterator iter = renderer->classificationAttributes().begin();
int classattr = *iter;
```

The Bug:

The serious bug occurs in the second line, where the iterator returned by the **classificationAttributes()** function is dereferenced:

```
int classattr = *iter;
```

According to the current ISO C++ Standard (draft), **iter** iterator is not dereferencable in that place, because the object of **std::list<int>** returned from the **classificationAttributes()** function is not available anymore. Simply, the usage of such iterator, after its parent object does not exist, causes **undefined behaviour**.

Where is this **undefined behaviour**?

```
std::list<int>::iterator iter = renderer->classificationAttributes().begin(); //<- r1
int classattr = *iter; //<- r2
```

In line (1), **classificationAttributes()** returns a list and this list is a temporary object. This object lives **only** untill the end of the

full-expression in which the object was created. So, it lives only till the end of the line (1). After the semicolon ending the expression in line (1), the list object is destroyed.
The iterator returned by **begin()** call in line (1) becomes *referencing to not existing object*. Next, in line (2) this iterator is dereferenced what causes **undefined behaviour**.

Here is what ISO C++ Standard says about temporary objects. This paragraph explains also why the list returned in the line (1) is destroyed.

12.2 Temporary objects

Temporary objects are destroyed as the last step in evaluating the
full-expression (1.9) that (lexically) contains the point where they
were created.

The statement **undefined behaviour** is very important here, because it explains why that buggy construction works with some compilers (like GCC) but with some it does not work (like VC++). Here is explanation of from ISO C++ Standard:

1.3.13 undefined behavior

[Note: permissible undefined behavior ranges from ignoring the situation completely with unpredictable results, to behaving during translation or program execution in a documented manner characteristic of the environment (with or without the issuance of a diagnostic message), to terminating a translation or execution (with the issuance of a diagnostic message). Many erroneous program constructs do not engender undefined behavior; they are required to be diagnosed. —end note]

There is no doubt this construction present in the constructor of **QgsUniqueValueDialog** causes **undefined behaviuor**.

Note: I grepped through all QGIS' .cpp files and then scanned all places where .begin() and .end() are used and I found two places where similar bug may occur, but I've not checked it yet. Here they are:

```
./plugins/gps_importer/qgsgpsplugin.cpp: iter != mQGisInterface->getLayerRegistry()->mapLayers().end(); ++iter) {
```

```
./plugins/gps_importer/qgsgpsplugin.cpp:  for (iter = mQGisInterface->getLayerRegistry()->mapLayers().begin();
```

Shortly, all places with so called chain access are suspicious and should be checked.

History

#1 - 2006-03-28 04:33 PM - Tim Sutton

- Resolution set to fixed

- Status changed from Open to Closed

Fixed in Trunk version commit:39a49242 (SVN r5106)

Thanks!

Tim

#2 - 2009-08-22 12:46 AM - Anonymous

Milestone Version 0.8 deleted

Files

qgsuniguevaluedialog.cpp-undefined-behaviour-fix-mloskot-20060329.patch	671 Bytes	2006-03-28	Mateusz Loskot -