QGIS Application - Bug report #21270
QGIS crashes when createInstance() uses wrong constructor in a QgsProcessingAlgorithm subclass
2019-02-14 01:59 PM - Reino Ruusu

| Status: | Closed |
| Priority: | High |
| Assignee: | Alessandro Pasotti |
| Category: | Processing/Core |
| Affected QGIS version: | 3.5(master) |
| Regression?: | No |
| Easy fix?: | No |
| Pull Request or Patch supplied: | Yes |
| Crashes QGIS or corrupts data: | Yes |
| Copied to github as #: | 29088 |

### Description

QGIS makes a hard crash when the createInstance() method calls a non-existent constructor in a python processing script class (QgsProcessingAlgorithm).

This is an easy error to make after creating a new script from a template.

### Reproduction

**Steps:**
- Create a new script in the Processing Toolbox using 'Create New Script from Template…'
- Rename class ExampleProcessingAlgorithm to anything else (such as MyProcessingAlgorithm). Leave reference to ExampleProcessingAlgorithm() in createInstance().
- Save template script
- Execute script by double-clicking it in Scripts/Example scripts/My script
- `:( QGIS Crashed` dialog

### Result

Crash ID: 4e33457d15a27ee43b8270be864ceb43b1208535

Stack Trace

```
QgsProcessingAlgorithm::setProvider :
QgsProcessingAlgorithm::create :
PyInit__core :
PyMethodDef_RawFastCallKeywords :
PyMethodDef_RawFastCallKeywords :
PyEval_EvalFrameDefault :
PyFunction_FastCallDict :
PyMethodDef_RawFastCallDict :
PyObject_Call :
PyInit_QtCore :
PyInit_QtCore :
PyInit_QtCore :
PyInit_QtCore :
PyInit_QtCore :
QMetaObject::activate :
QAbstractItemView::doubleClicked :
QTreeView::mouseDoubleClickEvent :
QWidget::event :
QFrame::event :
QAbstractItemView::viewportEvent :
QCoreApplicationPrivate::sendThroughObjectEventFilters :
QCoreApplicationPrivate::notify_helper :
QApplication::notify :
QgsApplication::notify :
QCoreApplication::notifyInternal2 :
```
QApplicationPrivate::sendMouseEvent:
QSizePolicy::QSizePolicy:
QSizePolicy::QSizePolicy:
QApplicationPrivate::notify_helper:
QApplication::notify:
QgsApplication::notify:
QCoreApplication::notifyInternal2:
QGuiApplicationPrivate::processMouseEvent:
QWindowSystemInterface::sendWindowSystemEvents:
QEventDispatcherWin32::processEvents:
CallWindowProcW:
DispatchMessageW:
QEventDispatcherWin32::processEvents:
qt_plugin_query_metadata:
QEventLoop::exec:
QCoreApplication::exec:
main:
BaseThreadInitThunk:
RtlUserThreadStart:

QGIS Info
QGIS Version: 3.4.4-Madeira
QGIS code revision: f6ddc62f6db
Compiled against Qt: 5.11.2
Running against Qt: 5.11.2
Compiled against GDAL: 2.4.0
Running against GDAL: 2.4.0

System Info
CPU Type: x86_64
Kernel Type: winnt
Kernel Version: 10.0.17134

Associated revisions
Revision 8db38af6b - 2019-02-18 03:21 PM - Alessandro Pasotti

Processing: fix crash in alg runner task with bad scripts

Fixes #21270

With test

History
#1 - 2019-02-16 10:54 AM - Giovanni Manghi
- Priority changed from Normal to High

#2 - 2019-02-18 02:47 PM - Alessandro Pasotti
- Assignee set to Alessandro Pasotti
- Operating System changed from Windows 10 Pro - build 17134.523 to Any
- Affected QGIS version changed from 3.4.4 to 3.5(master)

#3 - 2019-02-18 03:25 PM - Alessandro Pasotti
- Status changed from Open to In Progress
- Resolution set to fixed/implemented
- Pull Request or Patch supplied changed from No to Yes

2022-02-25
Btw, there are endless ways to crash QGIS from bad python code, we will never be able to prevent this to happen:
http://enki-editor.org/2014/08/23/Pyqt_mem_mgmt.html

#4 - 2019-02-20 07:43 AM - Alessandro Pasotti
- % Done changed from 0 to 100
- Status changed from In Progress to Closed

Applied in changeset commit:qgis|8db38af86d54b4481b23216ae13ed9cbcd8789b.