QGIS Application - Bug report #19989
QGIS crashes on Windows when loading and invalid KML file

2018-10-01 03:05 PM - Harry Clarke

Status:	Closed		
Priority:	High		
Assignee:	Even Rouault		
Category:	Data Provider/OGR		
Affected QGIS version:	3.3(master)	**Regression?:**	No
Operating System:	Windows	**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	up/downstream
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	27811

Description

User Feedback

Trying to load KML layer for
National Forest Inventory Woodland England

File downloaded from Forestry Commission website at
http://data-forestry.opendata.arcgis.com/datasets/national-forest-inventory-woodland-england?selectedAttribute=Shape_Leng

Report Details

Crash ID: e8c58a2f94d7f3fd2948b38a077a1a0795912c0c

Stack Trace

GDALReadWorldFile2 :
GDALAsyncReader::GetXSize :
GDALAsyncReader::GetXSize :
OGRCurveCollection::hasCurveGeometry :
OGRCurveCollection::hasCurveGeometry :
IGMLReader::~IGMLReader :
IGMLReader::~IGMLReader :
IGMLReader::~IGMLReader :
RegisterOGRLIBKML :
GDALOpenEx :
CPLStringList::FindString :
OGREnvelope::Merge :
std::basic_string<char,std::char_traits<char>,std::allocator<char> >::find_last_of :
std::basic_string<char,std::char_traits<char>,std::allocator<char> >::max_size :
OGREnvelope::OGREnvelope :
QgsProviderRegistry::createProvider :
QgsVectorLayer::setDataProvider :
QgsVectorLayer::setDataSource :
QgsVectorLayer::QgsVectorLayer :
QgisApp::addVectorLayer :
QgisApp::handleDropUriList :
CPLStringList::List :
QgisApp::identify :
QMetaObject::activate :
QTimer::timerEvent :
QObject::event :
QApplicationPrivate::notify_helper :
QApplication::notify :
QgsApplication::notify :
QCoreApplication::notifyInternal2 :
QEventDispatcherWin32Private::sendTimerEvent :
QEventDispatcherWin32::processEvents :
DispatchMessageW :
NotifyWinEvent :

QEventDispatcherWin32::processEvents :
qt_plugin_query_metadata :
QEventLoop::exec :
QCoreApplication::exec :
main :
BaseThreadInitThunk :
RtlUserThreadStart :

QGIS Info
QGIS Version: 3.2.3-Bonn
QGIS code revision: commit:9b176802e5
Compiled against Qt: 5.9.2
Running against Qt: 5.9.2
Compiled against GDAL: 2.2.4
Running against GDAL: 2.2.4

System Info
CPU Type: x86_64
Kernel Type: winnt
Kernel Version: 6.3.9600

History

#1 - 2018-10-02 10:26 AM - Giovanni Manghi

- Status changed from Open to Feedback

- Priority changed from Normal to High

- Category changed from Unknown to Data Provider/OGR

No crash here on master/linux. The KML (a whopping 2.1GB one) does not load. The QGIS logs says it is an invalid KML, in fact from the CLI ogr is clear about that:

giovanni@sibirica:~/Downloads$ ogrinfo -so National_Forest_Inventory_Woodland_England.kml
ERROR 4: ERROR parsing kml National_Forest_Inventory_Woodland_England.kml :invalid argument on line 1 at offset 0
ERROR 4: ERROR parsing kml National_Forest_Inventory_Woodland_England.kml :invalid argument on line 1 at offset 0
FAILURE:
Unable to open datasource `National_Forest_Inventory_Woodland_England.kml' with the following drivers.

#2 - 2018-10-02 08:52 PM - Harry Clarke

Seems like there is a difference in behaviour between Linux and Windows versions of QGIS, in that some error condition is not being trapped, which is resulting in QGIS crashing, rather than reporting an error with the input file.

#3 - 2018-10-03 02:43 PM - Giovanni Manghi

- Status changed from Feedback to Open

- Operating System changed from Windows 8.1 to Windows

- Affected QGIS version changed from 3.2.3 to 3.3(master)

- Subject changed from QGIS crash loading KML file to QGIS crashes on Windows when loading and invalid KML file

Confirmed on master/windows 10.

#4 - 2018-10-06 04:37 PM - Even Rouault

- Resolution set to up/downstream

- Status changed from Open to Closed

- Assignee set to Even Rouault

Didn't test on Windows, but could reproduce crashes on Linux with ogrinfo by limiting the process memory with ulimit -v

Fixes:

GDAL master: https://github.com/OSGeo/gdal/commit/bcd6e4e3595f951ecb516ad5d7572d401c838039

GDAL 2.3 branch: https://github.com/OSGeo/gdal/commit/06b46edb0f06c9b3217e6f9f1ea3cf1e38edcd02

Note: the KML is likely valid but both KML and LIBKML drivers need to ingest it completely in memory, so they choke on such huge files.