

## QGIS Application - Bug report #13002

### Crash opening GRASS 7 mapset in QGIS browser on Windows

2015-06-19 02:27 AM - Radim Blazek

<b>Status:</b>	Closed	
<b>Priority:</b>	Normal	
<b>Assignee:</b>	Radim Blazek	
<b>Category:</b>	GRASS	
<b>Affected QGIS version:</b>	2.8.2	<b>Regression?:</b> No
<b>Operating System:</b>	Windows	<b>Easy fix?:</b> No
<b>Pull Request or Patch supplied:</b>	No	<b>Resolution:</b>
<b>Crashes QGIS or corrupts data:</b>	Yes	<b>Copied to github as #:</b> 21079

#### Description

QGIS crashes when trying to expand a GRASS mapset with vectors using GRASS 7 provider on Windows (OSGeo4W). It works with GRASS 6 provider or if GRASS libs are compiled by MSVC instead of MinGW which is the case in OSGeo4W.

It crashes when functions are called on a FILE structure which was created by a library (libgrass\_gis.7.0.0.dll in this case) compiled by MinGW in a thread in QGIS by MSVC. It crashes in Microsoft

```
void __cdecl _lock_file (
    FILE *pf
)
{
    /*
     * The way the FILE (pointed to by pf) is locked depends on whether
     * it is part of _job[] or not
     */
    if ( (pf >= _job) && (pf <= (&_job[_IOB_ENTRIES-1])) )
    {
        /*
         * FILE lies in _job[] so the lock lies in _locktable[].
         */
        _lock( _STREAM_LOCKS + (int)(pf - _job) );
        /* We set _IOLOCKED to indicate we locked the stream */
        pf->_flag |= _IOLOCKED;
    }
    else
    {
        /*
         * Not part of _job[]. Therefore, *pf is a _FILEX and the
         * lock field of the struct is an initialized critical
         * section.
         */
        EnterCriticalSection( &(((_FILEX *)pf)->lock) );
    }
}
```

where \_FILEX is defined as

```
typedef struct {
    FILE f;
    CRITICAL_SECTION lock;
```

```
} _FILEX;
```

Most probably, when the file is opened in libgrass\_gis.7.0.0.dll compiled by MinGW, it is neither added to `_job[]` nor allocated as `_FILEX` but as `FILE` and accessing the lock is causing the crash.

## Associated revisions

**Revision cb7f9b4c - 2015-06-20 12:29 PM - Radim Blazek**

[GRASS] alloc enough space for Map\_info on Windows, fixes #13002

## History

**#1 - 2015-06-19 02:30 AM - Jürgen Fischer**

What calls `_lock_file`? I suppose somewhere on the path something passes a `FILE` pointer returned from one DLL to a function using `_lock_file` from another DLL and the two DLLs are not using the same version of `msvcrt` (or even something else).

**#2 - 2015-06-19 02:44 AM - Jürgen Fischer**

See also <https://lists.osgeo.org/pipermail/osgeo4w-dev/2015-June/002928.html>

**#3 - 2015-06-19 02:49 AM - Radim Blazek**

Even Rouault commented in mailing list:

*I cannot comment on this particular case, but in the Windows world, I believe the internal layout of FILE structure is specific to the C runtime used, so you cannot exchange them between different compilers. If you want to mix them, the library must return an opaque pointer to the using code and provide all needed functions to manipulate and free it.*

Which leads me to conclusion that I am probably on a wrong track.

The GRASS lib in fact does all the operations on the file. Because it is impossible to debug a lib compiled with MinGW when QGIS is compiled by MSVC and it works OK with GRASS libs compiled with MSVC I have mixed vector lib compiled by MSVC (which I can debug) with gis lib compiled by MinGW, which I thought is causing the problem.

**#4 - 2015-06-19 03:05 AM - Radim Blazek**

Jürgen Fischer wrote:

*What calls `_lock_file`? I suppose somewhere on the path something passes a FILE pointer returned from one DLL to a function using `_lock_file` from another DLL and the two DLLs are not using the same version of `msvcrt` (or even something else).*

Yes, my fault, I have mixed gis lib compiled by MinGW with vector lib compiled by MSVC.

The problem persists but the place where it really crashes will be different. Unfortunately I don't have any idea how to debug it. Traceback with GRASS libs compiled by MinGW is useless.

**#5 - 2015-06-19 05:40 AM - Radim Blazek**

I have also compiled GRASS 6.4.4 by MinGW myself in the same environment like GRASS 7.0.0 and it works without crash. It means that the problem is not caused by different compiler/options and it is probably something in GRASS 7 libs or in the provider code specific for GRASS 7.

**#6 - 2015-06-19 10:26 AM - Radim Blazek**

The provider (MSVC) calls Vect\_\_open\_old with struct Map\_info variable allocated in the provider where sizeof(struct Map\_info) = 1408. Vect\_\_open\_old (MinGW) calls G\_zero on that variable, where sizeof(struct Map\_info) = 1520.

It means that all structures used in GRASS libs must be also allocated in GRASS. New functions like Vect\_alloc\_map have to be added to GRASS and until it gets to GRASS and to OSGeo4w, the the structures must be be allocated in the provider with enough space.

Not yet fixed in source code.

**#7 - 2015-06-20 03:30 AM - Radim Blazek**

- *Status changed from Open to Closed*

Fixed in changeset commit:"cb7f9b4cf7f65632125c047ce8c319472a0ff728".