GROMACS - Bug #2465

Segmentation fault in mdrun because of file name lenght

03/23/2018 05:09 PM - Mikhail Serkov

Status:	Closed		
Priority:	Normal		
Assignee:	Berk Hess		
Category:	preprocessing (pdb2gmx,grompp)		
Target version:	2018.2		
Affected version - extra info:	ftp://ftp.gromacs.org/pub/gromacs/gromacs-2018.tar.gz	**Difficulty:**	uncategorized
Affected version:	2018		

Description

Hello,

I have recently found an issue when two of the tests were failing during the 'make check' with segmentation faults:

```
25 - GmxPreprocessTests (Child aborted)
     32 - MdrunTests (Child aborted)
```

It was really hard to reproduce, because it was only happening on our build environment (jenkins + easybuild). After debugging it appeared that this is happening because of path to the test file is too long. When you use jenkins + easybuild they create a really long folder tree.

During the debug, I found the reason why it is happening:
gromacs-2018/src/gromacs/fileio/warninp.cpp

```
typedef struct warninp {
    gmx_bool bAllowWarnings;
    int      nwarn_note;
    int      nwarn_warn;
    int      nwarn_error;
    int      maxwarn;
    int      lineno;
    char     filenm[256];
} t_warninp;
```

There is a declaration of warninp structure, and you may see that finlename size is *hardcoded* to be 256 characters. If the actual filename is more than 256, done_warning->free_warning->sfree->free causes segmentation fault.

I am not an expert in C++, I can't suggest how to make it more reliable. In my case I just patched the file and set it to 512, which resolved issue. However, it is only a workaround. Some additional handling is needed to check if filename is larger than this limit and throw an error, or set this filename to be dynamic buffer.

Please let me know if any questions.

Best regards,
Mikhail Serkov

Associated revisions

Revision 321dee2d - 04/03/2018 10:00 AM - Berk Hess

Change warninp filenm to std::string

This prevent buffer overflows with long filenames.

Fixes #2465

Change-Id: Ifcd264a6b33929f6b369d543c83c16d5378db937

History

#1 - 04/03/2018 10:00 AM - Gerrit Code Review Bot

Gerrit received a related patchset '1' for Issue #2465.
Uploader: Berk Hess (hess@kth.se)
Change-Id: gromacs~release-2018~Ifcd264a6b33929f6b369d543c83c16d5378db937
Gerrit URL: https://gerrit.gromacs.org/7744

#2 - 04/03/2018 10:01 AM - Berk Hess

- Category set to preprocessing (pdb2gmx,grompp)

- Status changed from New to Fix uploaded

- Assignee set to Berk Hess

- Target version set to 2018.2

#3 - 04/03/2018 12:00 PM - Berk Hess

- Status changed from Fix uploaded to Resolved

Applied in changeset 321dee2d032b85c9f620b0b7977e2e0fba464f20.

#4 - 04/03/2018 03:55 PM - Mark Abraham

- Status changed from Resolved to Closed

Will be fixed in 2018.2