GROMACS - Bug #2241

refdata can segfault when reading

09/04/2017 04:52 PM - Mark Abraham

Status:	New		
Priority:	Low		
Assignee:			
Category:	testing		
Target version:			
Affected version - extra info:		**Difficulty:**	uncategorized
Affected version:	git master		

Description

To reproduce, modify src/testutils/tests/refdata_tests.cpp case ReferenceDataTest HandlesIncorrectDataType to have name "Input Compound" rather than "Compound".

When reading a refdata xml file that contains a compound with a space in its name e.g. "Input Compound", the parsing result from tinyxml2 stops after "Input". I am not sure where the issue lies. To work around, don't use spaces in (at least) names of compounds.

Associated revisions

Revision 85e7dd18 - 09/12/2017 12:00 PM - Aleksei Iupinov

Prevent reference XML reader segfault on nullptr error strings

It is possible for TinyXML2 to return null pointers to the error strings.
This could cause XML reference data reader to segfault.

Refs #2241

Change-Id: I8b72917785080023f75388281dd2cbb4f30da925

History

#1 - 09/06/2017 05:24 PM - Gerrit Code Review Bot

Gerrit received a related patchset '1' for Issue #2241.
Uploader: Aleksei Iupinov (a.yupinov@gmail.com)
Change-Id: gromacs~master~I8b72917785080023f75388281dd2cbb4f30da925
Gerrit URL: https://gerrit.gromacs.org/6903

#2 - 09/06/2017 05:40 PM - Aleksei Iupinov

So the segfault happened because of our error handling as document.GetErrorStr2() was nullptr. document.GetErrorStr1() was just the rest of the XML.
I think that if you mean the first argument for checkCompound(), then that's an XML tag name itself, so it's not allowed to have space within. Not sure on the second one which is actually the value of the "Name" attribute.

#3 - 09/07/2017 11:57 AM - Mark Abraham

Aleksei Iupinov wrote:

> So the segfault happened because of our error handling as document.GetErrorStr2() was nullptr. document.GetErrorStr1() was just the rest of the XML.
> I think that if you mean the first argument for checkCompound(), then that's an XML tag name itself, so it's not allowed to have space within. Not sure on the second one which is actually the value of the "Name" attribute.

Hmm, its pretty scary that I forgot XML tag names cannot have spaces. TinyXML2 doesn't have much in the way of checking (ie "tiny") so perhaps we should save us from ourselves and check that one.