Buffer overflow in pdb2gmx with invalid r2b files

The function read_rtprename in pdb2gmx.c scans strings with sscanf into buffers of 6 chars. Residue and rtp names should be shorter than that, but any (invalid) input with longer strings will cause a buffer overflow and will cause pdb2gmx to segfault.

Associated revisions

Revision 501ce598 - 06/20/2015 08:10 PM - Erik Lindahl
Fix potential buffer overflow in pdb2gmx

Residue rename database entries were read into 6-char string variables. We now check and issue fatal errors if the lengths are above 5 characters.

Fixes #1649.

Change-Id: Id4d88a565b212ef279d400f42b5f2732550eded6

History

#1 - 12/09/2014 04:18 PM - Mark Abraham
- Target version changed from 5.0.3 to 5.0.4

#2 - 12/15/2014 09:46 PM - Mark Abraham
- Target version changed from 5.0.4 to 5.0.5

#3 - 05/06/2015 04:51 PM - Mark Abraham
- Target version changed from 5.0.5 to 5.0.6

#4 - 06/18/2015 02:47 PM - Gerrit Code Review Bot
Gerrit received a related patchset '1' for Issue #1649.
Uploader: Erik Lindahl (erik.lindahl@gmail.com)
Change-Id: l826539b706b14f3dbf938f5a56f48164faba164
Gerrit URL: https://gerrit.gromacs.org/4736

#5 - 06/18/2015 04:41 PM - Erik Lindahl
- Status changed from Accepted to Fix uploaded

#6 - 06/18/2015 06:52 PM - Gerrit Code Review Bot
Gerrit received a related patchset '1' for Issue #1649.
Uploader: Erik Lindahl (erik.lindahl@gmail.com)
Change-Id: l4d88a565b212ef279d400f42b5f2732550eded6
Gerrit URL: https://gerrit.gromacs.org/4740

#7 - 06/22/2015 12:39 PM - Rossen Apostolov
- Status changed from Fix uploaded to Closed