nice_header() in src/gmxlib/string2.c may dereference NULL pointer

07/09/2013 02:39 PM - Shun Sakuraba

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Mark Abraham</td>
</tr>
<tr>
<td>Category:</td>
<td>core library</td>
</tr>
<tr>
<td>Target version:</td>
<td>4.6.4</td>
</tr>
<tr>
<td>Affected version:</td>
<td>4.6.3</td>
</tr>
</tbody>
</table>

**Description**

If there exists pwd.h, but the user id cannot be found in password entry, getpwuid() returns NULL pointer. Since the user name is dereferenced without any test, this leads to null pointer dereference (and segmentation fault).

In src/gmxlib/string2.c,

```c
243 #ifdef HAVE_PWD_H
244   uid = getuid();
245   pw = getpwuid(uid);
246   gh = gethostname(buf, 255);
247   user = pw->pw_name;
248 #else
```

Fix is trivial:

```c
 user = (pw ? pw->pw_name : unk);```

**Associated revisions**

Revision Sc88c2b9 - 07/14/2013 05:28 AM - Mark Abraham

Fixed possible dereference of null pointer

getpwuid() can return null. For example, Shun Sakuruba reported that on Cray XE6 compute nodes have passwd.h, but users will not have passwd entries.

Fixes #1301

Change-id: I66e8064438fc02591629b0d381bc00af6795c0

**History**

#1 - 07/11/2013 08:45 AM - Shun Sakuraba

Note: the problem happened on Cray XE6 system, where the "compute nodes" do not have password entry of users.

#2 - 07/12/2013 01:44 AM - Mark Abraham

- Status changed from New to Fix uploaded
- Target version set to 4.6.4

Thanks https://gerrit.gromacs.org/2497

#3 - 08/13/2013 08:55 PM - Mark Abraham

- Status changed from Fix uploaded to Resolved
- % Done changed from 0 to 100
Applied in changeset 5c88c2b958efcf979e47ba04e1480ac04baa773.

#4 - 10/17/2013 05:58 PM - Mark Abraham

- Status changed from Resolved to Closed