Charm++ - Bug #1448
Potential buffer overflow in mylogin()
02/27/2017 04:28 PM - Matthias Diener

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
<th>Start date:</th>
<th>02/27/2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Low</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>Matthias Diener</td>
<td>% Done:</td>
<td>0%</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
<td>Spent time:</td>
<td>0.00 hour</td>
</tr>
</tbody>
</table>

Description
There is a potential buffer overflow in mylogin() when having a long username

```c
char uname[64];
sprintf(cmd, "id -u -n");
p = popen(cmd, "r");
if (p) {
    fscanf(p, "%s", uname);
```

If the username is longer than 64 characters, it will overwrite the uname variable. Current systems support usernames of at least 256 characters (test with getconf LOGIN_NAME_MAX).

I can see two ways to fix this:
- Completely remove the #if CMK_HAS_POPEN case.
- Replace with getline()/strdup().