Subject: [PATCH 01/14] sysfs: fix i_mutex locking in sysfs_get_dentry()
Posted by Tejun Heo on Mon, 20 Aug 2007 12:36:29 GMT
View Forum Message <> Reply to Message

lookup_one_len_kern() should be called with the parent's i_mutex
locked. Fix it.

Spotted by Eric W. Biederman.

Signed-off-by: Tejun Heo <htejun@gmail.com>
Cc: Eric W. Biederman <ebiederm@xmission.com>
---
 fs/sysfs/dir.c | 2 ++
 1 files changed, 2 insertions(+), 0 deletions(-)

diff --git a/fs/sysfs/dir.c b/fs/sysfs/dir.c
index e4fd8a2..b33af5e 100644
--- a/fs/sysfs/dir.c
+++ b/fs/sysfs/dir.c
@@ -130,8 +130,10 @@ struct dentry *sysfs_get_dentry(struct sysfs_dirent *sd)

   /* look it up */
   parent_dentry = dentry;
+ mutex_lock(&parent_dentry->d_inode->i_mutex);
   dentry = lookup_one_len_kern(cur->s_name, parent_dentry,
          strlen(cur->s_name));
+ mutex_unlock(&parent_dentry->d_inode->i_mutex);
   dput(parent_dentry);

   if (IS_ERR(dentry)) {
--
1.5.0.3

_____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers