Subject: [patch 2.6.21-rc3] [smbfs] "double free" memory corruption in smbfs
Posted by vaverin on Wed, 14 Mar 2007 12:23:33 GMT
View Forum Message <> Reply to Message

smbfs allocates rq_trans2buffer to handle server's multi transaction2 response
messages. As struct smb_request may be reused, rq_trans2buffer is freed before
each new request. However if last servers's response is not multi but single
trans2 message then new rq_trans2buffer is not allocated but last smb_rput still
tries to free it again.
To prevent this issue rq_trans2buffer pointer should be set to NULL after kfree.

Signed-off-by: Vasily Averin <vvs@sw.ru>

```
--- 2.6.21-rc3/fs/smbfs/request.c 2007-03-13 14:22:53.000000000 +0300
+++ 2.6.21-rc3/fs/smbfs/request.c 2007-03-14 11:44:18.000000000 +0300
@@ -181,6 +181,7 @@ static int smb_setup_request(struct smb_
  req->rq_errno = 0;
  req->rq_fragment = 0;
  kfree(req->rq_trans2buffer);
+ req->rq_trans2buffer = NULL;

  return 0;
 }
```