
Subject: Re: [PATCH] Correct accept(2) recovery after sock_attach_fd()

Posted by [davem](#) on Mon, 26 Mar 2007 21:20:20 GMT

[View Forum Message](#) <> [Reply to Message](#)

From: Alexey Dobriyan <adobriyan@sw.ru>

Date: Mon, 26 Mar 2007 19:34:31 +0400

> * d_alloc() in sock_attach_fd() fails leaving ->f_dentry of new file NULL

> * bail out to out_fd label, doing fput()/__fput() on new file

> * but __fput() assumes valid ->f_dentry and dereferences it

>

> Signed-off-by: Alexey Dobriyan <adobriyan@sw.ru>

Thanks for this bug fix Alexey, patch applied.
