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

Posted by [Alexey Dobriyan](#) on Mon, 26 Mar 2007 15:26:44 GMT

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

- * 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>

net/socket.c | 7 ++++++-
1 file changed, 6 insertions(+), 1 deletion(-)

--- a/net/socket.c

+++ b/net/socket.c

@@ -1381,7 +1381,7 @@ asmlinkage long sys_accept(int fd, struc

```
    err = sock_attach_fd(newsock, newfile);  
    if (err < 0)  
-    goto out_fd;  
+    goto out_fd_simple;
```

```
    err = security_socket_accept(sock, newsock);  
    if (err)  
@@ -1414,6 +1414,11 @@ out_put:  
    fput_light(sock->file, fput_needed);  
out:  
    return err;
```

```
+out_fd_simple:  
+    sock_release(newsock);  
+    put_filp(newfile);  
+    put_unused_fd(newfd);  
+    goto out_put;  
out_fd:  
    fput(newfile);  
    put_unused_fd(newfd);
```

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.
