
Subject: Re: [PATCH 1/4] proc: fix NULL ->i_fop oops
Posted by [Christoph Hellwig](#) on Tue, 20 Nov 2007 15:17:31 GMT
[View Forum Message](#) <> [Reply to Message](#)

On Tue, Nov 20, 2007 at 10:05:05AM -0500, Stephen Smalley wrote:

> > Nice, getting rid of this is a very good step formwards. Unfortunately
> > we have another copy of this junk in
> > security/selinux/selinuxfs.c:sel_remove_entries() which would need the
> > same treatment.
>
> Can't just be dropped completely for selinux - we need a way to drop
> obsolete entries from the prior policy when we load a new policy.
>
> Is the only real problem here the clearing of f_op? If so, we can
> likely remove that from sel_remove_entries() without harm, and fix the
> checks for it to use something more reliable.

f_op removal is the biggest issue. It can't really work and this is the last instance. But in general having some half-backed attempts at revoke is never a good idea.
