

---

Subject: Re: [PATCH 1/4] proc: fix NULL ->i\_fop oops  
Posted by [Christoph Hellwig](#) on Mon, 19 Nov 2007 12:51:39 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

On Fri, Nov 16, 2007 at 06:06:51PM +0300, Alexey Dobriyan wrote:  
> proc\_kill\_inodes() can clear ->i\_fop in the middle of vfs\_readdir resulting in  
> NULL dereference during "file->f\_op->readdir(file, buf, filler)".  
>  
> The solution is to remove proc\_kill\_inodes() completely:  
> a) we don't have tricky modules implementing their tricky readdir hooks which  
> could keep this revoke from hell.  
> b) In a situation when module is gone but PDE still alive, standard readdir  
> will return only "." and "..", because pde->next was cleared by  
> remove\_proc\_entry().  
> c) the race proc\_kill\_inode() destined to prevent is not completely fixed, just  
> race window made smaller, because vfs\_readdir() is run without sb\_lock held and  
> without file\_list\_lock held. Effectively, ->i\_fop is cleared at random moment,  
> which can't fix properly anything.

Nice, getting rid of this is a very good step forwards. Unfortunately  
we have another copy of this junk in  
security/selinux/selinuxfs.c:sel\_remove\_entries() which would need the  
same treatment.

---