
Subject: Re: [patch 0/8] unprivileged mount syscall
Posted by [Ian Kent](#) on Wed, 11 Apr 2007 13:48:30 GMT
[View Forum Message](#) <> [Reply to Message](#)

On Wed, 2007-04-11 at 12:48 +0200, Miklos Szeredi wrote:

> > > >
> > > > - users can use bind mounts without having to pre-configure them in
> > > > /etc/fstab
> > > >
> > >
> > > This is by far the biggest concern I see. I think the security
> > > implication of allowing anyone to do bind mounts are poorly understood.
> >
> > And especially so since there is no way for a filesystem module to veto
> > such requests.
>
> The filesystem can't veto initial mounts based on destination either.
> I don't think it's up to the filesystem to police bind/move mounts in
> any way.

But if a filesystem can't or the developer thinks that it shouldn't for some reason, support bind/move mounts then there should be a way for the filesystem to tell the kernel that.

Surely a filesystem is in a good position to be able to decide if a mount request "for it" should be allowed to continue based on it's "own situation and capabilities".

Ian

Containers mailing list
Containers@lists.linux-foundation.org
<https://lists.linux-foundation.org/mailman/listinfo/containers>
