
Subject: Re: [patch] unprivileged mounts update
Posted by [serge](#) on Wed, 25 Apr 2007 18:52:44 GMT
[View Forum Message](#) <> [Reply to Message](#)

Quoting Eric W. Biederman (ebiederm@xmission.com):

> "Serge E. Hallyn" <serge@hallyn.com> writes:
>
> > Quoting Eric W. Biederman (ebiederm@xmission.com):
> >>
> >> Are there other permission checks that mount is doing that we
> >> care about.
> >
> > Not mount itself, but in looking up /share/fa/root/home/fa,
> > user fa doesn't have the rights to read /share, and by setting
> > fsuid to fa and dropping CAP_DAC_READ_SEARCH the mount action fails.
>
> Got it.
>
> I'm not certain this is actually a problem it may be a feature.
> But it does fly in the face of the general principle of just
> getting out of roots way so things can get done.
>
> I think we can solve your basic problem by simply doing like:
> chdir(/share); mount(.); To simply avoid the permission problem.
>
> The practical question is how much do we care.
>
> > But the solution you outlined in your previous post would work around
> > this perfectly.
>
> If we are not using usual permissions which user do we use current->uid?
> Or do we pass that user someplace?

Right, I figure if the normal action is to always do
mnt->user = current->fsuid, then for the special case we
pass a uid in someplace. Of course... do we not have a
place to do that? Would it be a no-no to use 'data' for
a non-fs-specific arg?

> >> > If it were really the equivalent then I could keep my capabilities :)
> >> > after changing it.
> >>
> >> We drop all capabilities after we change the euid.
> >
> > Not if we've done prctl(PR_SET_KEEPCAPS, 1)
>
> Ah cap_clear doesn't do the obvious thing.
>

> Eric

Containers mailing list

Containers@lists.linux-foundation.org

<https://lists.linux-foundation.org/mailman/listinfo/containers>
