Subject: Re: [patch 0/8] unprivileged mount syscall
Posted by hpa on Sat, 07 Apr 2007 00:22:49 GMT
View Forum Message <> Reply to Message

Jan Engelhardt wrote:
> On Apr 6 2007 16:16, H. Peter Anvin 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.
>
> $ whoami
> miklos
> $ mount --bind / ~/down_under
>
> later that day:
> # userdel -r miklos
>
> So both the source (/) and target (~/down_under) directory must be owned
> by the user before --bind may succeed.
>
> There may be other implications hpa might want to fill us in.

Consider backups, for example.

 -hpa

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

Subject: Re: [patch 0/8] unprivileged mount syscall
Posted by Eric Van Hensbergen on Sat, 07 Apr 2007 03:40:20 GMT
View Forum Message <> Reply to Message

On 4/6/07, H. Peter Anvin <hpa@zytor.com> wrote:
> Jan Engelhardt wrote:
> > On Apr 6 2007 16:16, H. Peter Anvin 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.
> >
> > $ whoami
> > miklos

> > $ mount --bind / ~/down_under
> >
> > later that day:
> > # userdel -r miklos
> >
>
> Consider backups, for example.
>

This is the reason why enforcing private namespaces for user mounts
makes sense. I think it catches many of these corner cases.

-eric

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

---

Subject: Re: [patch 0/8] unprivileged mount syscall
Posted by Miklos Szeredi on Sat, 07 Apr 2007 06:48:20 GMT
View Forum Message <> Reply to Message

> On 4/6/07, H. Peter Anvin <hpa@zytor.com> wrote:
> > Jan Engelhardt wrote:
> > > On Apr 6 2007 16:16, H. Peter Anvin 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.
> > >
> > > $ whoami
> > > miklos
> > > $ mount --bind / ~/down_under
> > >
> > > later that day:
> > > # userdel -r miklos
> > >
> >
> > Consider backups, for example.
> >
>
> This is the reason why enforcing private namespaces for user mounts
> makes sense. I think it catches many of these corner cases.

Yes, disabling user bind mounts in the global namespace makes sense.

Enabling user fuse mounts in the global namespace still works though,
even if a little cludgy. All these nasty corner cases have been
thought through and validated by a lot of users.

Thanks,
Miklos

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