Subject: Re: [patch 7/9] unprivileged mounts: allow unprivileged fuse mounts
Posted by Miklos Szeredi on Wed, 09 Jan 2008 09:11:06 GMT
View Forum Message <> Reply to Message

> > > 'updatedb no longer works' is not a problem?
> >
> > I haven't seen any problems with updatedb, and haven't had any bug
> > reports about it either.
>
> Ok, I don't know much about FUSE. In current version, if user creates
> infinite maze and mounts it under ~, updatedb just does not enter it?

It doesn't. See Documentation/filesystems/fuse.txt

> > AFAIR there were two security vulnerabilities in fuse's history, one
> > of them an information leak in the kernel module, and the other one an
> > mtab corruption issue in the fusermount utility. I don't think this
> > is such a bad track record.
>
> Not bad indeed. But I'd consider 'kill -9 not working' to be DoS
> vulnerability...

The worst that can happen is that a sysadmin doesn't read the docs (likely) before enabling fuse on a multiuser system, and is surprised by a user doing funny things. And _then_ has to go read the docs, or google for some info. This is basically how things normally work, and I don't consider it a DoS.

> and I'm woried about problems fuse + user mounts expose in other
> parts of system.

I'm worried too, and I'm not saying that enabling unprivileged fuse mounts is completely risk free. Nothing is, and nobody is forced to do it.

Miklos

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