
Subject: Re: [patch 7/9] unprivileged mounts: allow unprivileged fuse mounts
Posted by [Pavel Machek](#) on Tue, 08 Jan 2008 22:58:20 GMT

[View Forum Message](#) <> [Reply to Message](#)

On Tue 2008-01-08 23:42:20, Miklos Szeredi wrote:

> > On Tue 2008-01-08 12:35:09, Miklos Szeredi wrote:

> > > From: Miklos Szeredi <mszeredi@suse.cz>

> > >

> > > Use FS_SAFE for "fuse" fs type, but not for "fuseblk".

> > >

> > > FUSE was designed from the beginning to be safe for unprivileged users. This

> > > has also been verified in practice over many years. In addition unprivileged

> >

> > Eh? So 'kill -9 no longer works' and 'suspend no longer works' is not

> > considered important enough to even mention?

>

> No. Because in practice they don't seem to matter. Also because

> there's no way in which fuse could be done differently to address

> these issues.

>

> The 'kill -9' thing is basically due to VFS level locking not being

> interruptible. It could be changed, but I'm not sure it's worth it.

Well, I believe it should be changed. "You need to mount /sys, then
echo X to Y before kill -9 works" does not look nice... I agree it is
not easy.

> > '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?

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

Pavel

--

(english) <http://www.livejournal.com/~pavelmachek>

(cesky, pictures) <http://atrey.karlin.mff.cuni.cz/~pavel/picture/horses/blog.html>

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