
Subject: Re: [patch 6/9] unprivileged mounts: allow unprivileged mounts

Posted by [Karel Zak](#) on Wed, 09 Jan 2008 11:11:20 GMT

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

On Tue, Jan 08, 2008 at 12:35:08PM +0100, Miklos Szeredi wrote:

> Define a new fs flag FS_SAFE, which denotes, that unprivileged mounting of
> this filesystem may not constitute a security problem.

>

> Since most filesystems haven't been designed with unprivileged mounting in
> mind, a thorough audit is needed before setting this flag.

>

> For "safe" filesystems also allow unprivileged forced unmounting.

What about to list "safe" filesystems anywhere in /proc/fs/ ? I think
it's very important information for admins.

Note, your patch for mount(8) is always trying to use unprivileged
mount(2) for non-root users. It's overkill when unprivileged mounts are
supported for bind mounts and fuse only. It would be nice to check
if FS is "safe" before switch to unprivileged mode.

The "safe" definition is also very subjective and it depends on your
level of paranoia. There should be a way (e.g. /proc) how control and
modify the list of "safe" filesystems. For example I have no problem
to mark cifs as "safe" for my home server.

Karel

--

Karel Zak <kzak@redhat.com>

Containers mailing list

Containers@lists.linux-foundation.org

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