Subject: Re: [patch 7/8] allow unprivileged mounts
Posted by ebiederm on Sat, 21 Apr 2007 16:57:10 GMT
View Forum Message <> Reply to Message

Jan Engelhardt <jengelh@linux01.gwdg.de> writes:

> On Apr 21 2007 08:10, Eric W. Biederman 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.
>>>
>>> Practically speaking, is there any realistic likelihood that any filesystem
>>> apart from FUSE will ever use this?
>>
>>Also potentially some of the kernel virtual filesystems. /proc should
>>be safe already. If you don't have any kind of backing store this problem
>>gets easier.
>
> tmpfs!

tmpfs is a possible problem because it can consume lots of ram/swap. Which
is why it has limits on the amount of space it can consume. Those are set as
mount options as I recall. Which means that we would need to do something
different with respect to limits before tmpfs could become safe for
an untrusted user to mount.

Still it's close.

Eric

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