

---

Subject: Re: [patch 0/8] unprivileged mount syscall  
Posted by [Miklos Szeredi](#) on Mon, 16 Apr 2007 09:27:45 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

> Arn't there ways to escape chroot jails? Serge had pointed me to a URL  
> which showed chroots can be escaped. And if that is true than having all  
> user's private mount tree in the same namespace can be a security issue?

No. In fact chrooting the user into /share/\$USER will actually  
\_grant\_ a privilege to the user, instead of taking it away. It allows  
the user to modify it's root namespace, which it wouldn't be able to  
in the initial namespace.

So even if the user could escape from the chroot (which I doubt), s/he  
would not be able to do any harm, since unprivileged mounting would be  
restricted to /share. Also /share/\$USER should only have read/search  
permission for \$USER or no permissions at all, which would mean, that  
other users' namespaces would be safe from tampering as well.

Miklos

---

Containers mailing list  
[Containers@lists.linux-foundation.org](mailto:Containers@lists.linux-foundation.org)  
<https://lists.linux-foundation.org/mailman/listinfo/containers>

---