Subject: Re: [patch 0/8] mount ownership and unprivileged mount syscall (v4)
Posted by ebiederm on Wed, 25 Apr 2007 01:04:36 GMT
View Forum Message <> Reply to Message

Karel Zak <kzak@redhat.com> writes:

> On Fri, Apr 20, 2007 at 12:25:32PM +0200, Miklos Szeredi wrote:
>> The following extra security measures are taken for unprivileged
>> mounts:
>>
>> - usermounts are limited by a sysctl tunable
>> - force "nosuid,nodev" mount options on the created mount
>
> The original userspace "user=" solution also implies the "noexec"
> option by default (you can override the default by "exec" option).
>
> It means the kernel based solution is not fully compatible ;-(

Why noexec? Either it was a silly or arbitrary decision, or
our kernel design may be incomplete.

Now I can see not wanting to support executables if you are locking
down a system. The classic don't execute a program from a CD just because
the CD was stuck in the drive problem.

So I can see how executing code from an untrusted source could prevent
exploitation of other problems, and we certainly don't want to do it
automatically.

Eric

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