Subject: Re: [RFC][PATCH 0/2] user namespace [try #2]
Posted by ebiederm on Mon, 11 Sep 2006 11:48:25 GMT
View Forum Message <> Reply to Message

Cedric Le Goater <clg@fr.ibm.com> writes:

> Eric W. Biederman wrote:
>> Herbert Poetzl <herbert@13thfloor.at> writes:
>>
>>
>> In addition I don't have problems with incremental progress
>> if we implement in such a way that we don't enable the ability
>> to create a new uid namespace to user space before we are certain
>> it is safe.
>>
>> All of the code could be present and we just have a one line check
>> that denied requests to create a new namespace.
>
> OK. I'll see how this is possible. I guess the simplest way for the moment
> is to remove the unshare() of the user_namespace.

That is largely what I was thinking. Possibly even leaving the code
there but denying all requests with the CLONE_NEWUSERNS bit set.

> So, shall we follow the 'grep' method for uids like we are doing for pids
> and thread ? This is going to be painful but I guess there is no simple
> solution ...

I can't think of a better one. Although hopefully since security
is involved those checks are in a little better shape, and a little
less distributed throughout the kernel.

Eric

_____
Containers mailing list
Containers@lists.osdl.org
https://lists.osdl.org/mailman/listinfo/containers