Subject: Re: Re: [RFC][PATCH 0/2] user namespace [try #2]
Posted by dev on Thu, 07 Sep 2006 16:06:26 GMT
View Forum Message <> Reply to Message

Cedric Le Goater wrote:
> Eric W. Biederman wrote:
>
>>Cedric Le Goater <clg@fr.ibm.com> writes:
>>
>>
>>>Eric W. Biederman wrote:
>>>
>>>[...]
>>>
>>>
>>>>Cedric sorry for not saying so earlier, but I thought that the incompleteness
>>>>was obvious.
>>>
>>>No worries :) But let's see how obvious is that incompleteness before we
>>>add more work to it.
>>
>>Sorry I don't understand what you mean.
>>Are you suggesting not fixing bugs because everyone cannot see them?
>
>
> I'm only suggesting to wait for the opinion of the vserver and openvz guys.
>
> If it's already useful for someone, good. if not, let's work on it when we
> have time. if they are bugs, let's fix them.
yes, these patches are usable for OpenVZ AS IS, so I'm not sure
why we can't do step by step and commit. However I posted some comments on patches...

Eric do you have some STRONG objections (maybe I just missed it somewhere)?

Thanks,
Kirill

Subject: Re: [RFC][PATCH 0/2] user namespace [try #2]
Posted by ebiederm on Thu, 07 Sep 2006 18:18:14 GMT
View Forum Message <> Reply to Message

Kirill Korotaev <dev@sw.ru> writes:

> yes, these patches are usable for OpenVZ AS IS, so I'm not sure
> why we can't do step by step and commit. However I posted some comments on
> patches...
>

> Eric do you have some STRONG objections (maybe I just missed it somewhere)?

- We do not handle interactions between processes in different uid namespaces
  and still have the normal uid equality checks.
- I am willing to be convinced that this is a nuclear missile the user is
  allowed to shoot themselves in the foot with if someone can show me how
  to use the current version safely.

A lot of this scares me silly as when ever you touch the primary identifier
in the security checks you must be very very very careful. My gut feeling
is that I'm nowhere near paranoid enough and the rest of you aren't even
paranoid.

What I want to see is that every uid identity check becomes either
a struct user comparison or a uid, uid_ns tuple comparison.

Eric

Subject: Re: [RFC][PATCH 0/2] user namespace [try #2]
Posted by Herbert Poetzl on Thu, 07 Sep 2006 18:30:46 GMT
View Forum Message <> Reply to Message

On Thu, Sep 07, 2006 at 12:18:14PM -0600, Eric W. Biederman wrote:
> Kirill Korotaev <dev@sw.ru> writes:
>
> > > yes, these patches are usable for OpenVZ AS IS, so I'm not sure
> > > why we can't do step by step and commit. However I posted some comments on
> > > patches...
> > >
> > > Eric do you have some STRONG objections (maybe I just missed it somewhere)?
>
> - We do not handle interactions between processes in different uid
>   namespaces and still have the normal uid equality checks.
> - I am willing to be convinced that this is a nuclear missile the user
>   is allowed to shoot themselves in the foot with if someone can show me
>   how to use the current version safely.
>
> A lot of this scares me silly as when ever you touch the primary
> identifier in the security checks you must be very very very careful.
> My gut feeling is that I'm nowhere near paranoid enough and the rest
> of you aren't even paranoid.
>
> What I want to see is that every uid identity check becomes either
> a struct user comparison or a uid, uid_ns tuple comparison.

second that!

best,
Herbert

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

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