Subject: Re: [PATCH 2/2] Fix user namespace exiting OOPs
Posted by Pavel Emelianov on Mon, 17 Sep 2007 06:21:53 GMT
View Forum Message <> Reply to Message

Andrew Morton wrote:
> On Fri, 14 Sep 2007 13:23:55 -0500 "Serge E. Hallyn" <serue@us.ibm.com> wrote:
>
>>> run on kernel with CONFIG_USER_NS turned on will oops the
>>> kernel immediately.
>>>
>>> This was spotted during OpenVZ kernel testing.
>>>
>>> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>
>>> Signed-off-by: Alexey Dobriyan <adobriyan@openvz.org>
>> Good spot. Interesting solution :)
>>
>
> Do we want to fix this in 2.6.23?

This is not a security issue at all. This BUG can be triggered only
by CAP_SYS_ADMIN capable task on the kernel with CONFIG_USER_NS=y,
which is an EXPERIMENTAL depending option.

> If so then at present I'll need to merge
>
> kernel-userc-use-list_for_each_entry-instead-of-list_for_each.patch
> convert-uid-hash-to-hlist.patch
> fix-user-namespace-exiting-oops.patch
>
> which is rather a lot of merging at this stage - surely more than
> is really needed?
>

Thanks,
Pavel