Subject: ATTENTION you can get root on x64 - Zero extend all registers after ptrace in 32bit entry path.
Posted by disaster on Sat, 29 Sep 2007 09:49:01 GMT
View Forum Message <> Reply to Message

Hello!

Isn't this one http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.20.y.git;a=commitdiff;h=0d4a39318e6177ed424e92fe9ea75b514e782cdc also related to openvz Kernel? I mean you can get root rights with it in a VPS or as a user on the Host if it is a x64 build.

Subject: Re: Zero extend all registers after ptrace in 32bit entry path.
Posted by disaster on Sat, 29 Sep 2007 14:17:40 GMT
View Forum Message <> Reply to Message

It is relevant - everyone can get root access. Apply the patch from 2.6.20 in the link to your 2.6.18 kernel - it fixes the problem (only some hunks).

Subject: Re: Zero extend all registers after ptrace in 32bit entry path.
Posted by dev on Wed, 24 Oct 2007 14:54:53 GMT
View Forum Message <> Reply to Message

1. better send such notices to devel@openvz.org (it can help just in case we missed something)
2. just for info: it was fixed in 028stab045