Subject: *CLOSED* Security breach :: prctl vulnerability
Posted by whatever on Thu, 12 Oct 2006 17:54:49 GMT
View Forum Message <> Reply to Message

How is it possible the VPS owner break into main node?
I am shocked. Is openVZ really safe at all?
Anyway I can check how it was done and how it can be avoided in future?
Can anyone help me with this??????

Thanks.

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by Vasily Tarasov on Fri, 13 Oct 2006 05:20:38 GMT
View Forum Message <> Reply to Message

It should be impossible!

Please, tell us, how do you detect, that a user from VE break into HN?

Thanks!

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by John Kelly on Fri, 13 Oct 2006 15:05:33 GMT
View Forum Message <> Reply to Message

whatever wrote on Thu, 12 October 2006 13:54How is it possible the VPS owner break into main node?

The VE has a chrooted, limited view of the filesystem. So the VE cannot "break in" to the HN filesystem.

However, the VE can use ssh to login to the HN, just like any other networked host. Maybe you have poor security on your HN. But how can we know what happened, when you don't provide detailed, factual information?

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by whatever on Fri, 13 Oct 2006 16:01:59 GMT
View Forum Message <> Reply to Message

How I detected?
In hardware node we use alert script whenever anyone login to root we get alert. And direct root

login to Hardware node is disabled. To get root access one has to login as user allowed list in hardware node and then su password to get root.
There are only 2 users in hardware.
The VPS user got the access to root. And the details of VPSuser, ip, time etc were recorded in alert email.
This happened 2 times with different VPS users.
I can send the VPS root access and alert details to the developer of openvz to have a look at it.
Maybe they can understand better then me.

Thanks.

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by John Kelly on Fri, 13 Oct 2006 16:29:09 GMT
View Forum Message <> Reply to Message

whatever wrote on Fri, 13 October 2006 12:01And direct root login to Hardware node is disabled.

Maybe. Maybe not. It's possible there could be an OpenVZ bug, but it's more likely your login security is misconfigured.

If you can identify a real bug, the OpenVZ developers will fix it. That's their job. But they don't have time, and it's not their job, to train OpenVZ users how to manage system security.

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by whatever on Sat, 14 Oct 2006 12:14:23 GMT
View Forum Message <> Reply to Message

There are more people who have faced this issue.
one other guy got his access with this code
http://www.milw0rm.com/exploits/2006

Thanks

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by jason|xoxide on Sun, 15 Oct 2006 14:20:10 GMT
View Forum Message <> Reply to Message

Well, if it's a kernel bug that only affects 2.6.17 and below then it will go away as soon as the test kernel is migrated to 2.6.18 (which they already said would be soon). You can't very well blame OpenVZ for something that is also broken in the vanilla kernel.

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by Valmont on Sun, 15 Oct 2006 14:37:25 GMT
View Forum Message <> Reply to Message

You are mistaken. It can gives root access, but does _not_ break vps restrictions.

And. Do NOT use testing kernel on production. It is only for testing purposes. Use stable kernel.

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by whatever on Sun, 15 Oct 2006 15:18:54 GMT
View Forum Message <> Reply to Message

I am using kernel

kernel /vmlinuz-2.6.8-022stab078.10 ro root=/dev/VolGroup00/LogVol00

Thanks

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by Valmont on Sun, 15 Oct 2006 15:52:33 GMT
View Forum Message <> Reply to Message

Well, did you try to execute this sploit?
It doesn't work on 2.6.8-022stab078.10

Subject: Re: Security breach :: VPS owner break into main node!!!!
Posted by dev on Tue, 17 Oct 2006 10:46:09 GMT
View Forum Message <> Reply to Message

2.6.8 stable is not vulnerable since prctl was broken between 2.6.8 and 2.6.9.

2.6.9 stable was updated some time ago (linux-2.6.9-CVE-2006-2451-dumpable.patch)

Plus as someone already noted here, this doesn't allow to get HWN root user. Only VE root.