Subject: User ID's and OpenVZ - something you should really consider fixing
Posted by devonblzx on Mon, 15 Oct 2007 20:00:16 GMT
View Forum Message <> Reply to Message

Something I noticed today. I have been running under OpenVZ for a while now and have not run into any main issues but recently I was running commands under a user I made on the main node and when I typed killall -9 process, I thought all was well because it was just a regular user nothing bad should have happened. Little did I know the way OpenVZ reads the user ID's. Apparently when I ran that under my user (user id 501) it killed every single kind of the process in the VPS's who had them running under user ID 501. It was a screen that I killed and I could not figure out why it was happening to this user until I decided to do a ps on the system.

When I ran the "ps ax | grep user" it showed up as my username owning all the processes inside of the VPS's owned by user 501. This means my regular user had access to kill every single process running under that UID inside any VPS.

I guess I had never noticed this before because I don't usually do much with my username on the VPS nodes but this just doesn't seem very secure.

Subject: Re: User ID's and OpenVZ - something you should really consider fixing
Posted by rickb on Mon, 15 Oct 2007 20:08:03 GMT
View Forum Message <> Reply to Message

http://forum.openvz.org/index.php?t=tree&th=592&mid= 3206&&rev=&reveal=

http://openvz-mirror1.rapidvps.com/contrib/kernel-patches/di ff-ve0-proc-own-processes-only