Subject: OpenVZ mounting /proc insecurely
Posted by curtis_isparks on Tue, 06 Oct 2015 20:40:50 GMT

I recently discovered that the way OpenVZ mounts /proc inside of containers by default is insecure. The following article describes how to fix the issue on the host node:

https://lwn.net/Articles/191531/

However, this does not work inside of containers. At least it doesn't anymore. Under Proxmox 1.9 (vzkernel-2.6.32-042stab037.1) I could do this:

mount -o remount,nosuid,noexec /proc

But, now I'm running OpenVZ under Proxmox 3.1 (vzkernel-2.6.32-042stab079.5) and this no longer works:

mount -o remount,nosuid,noexec /proc
mount: mount failed

In LXC I noticed that /proc attributes can be specified using the lxc.mount.auto configuration option in the container config. I haven't been able to figure out how to do this in OpenVZ. Any ideas?