Subject: Re: [PATCH 6/7]: Check for user-space mount of /dev/pts
Posted by Sukadev Bhattiprolu on Tue, 25 Mar 2008 17:25:45 GMT
View Forum Message <> Reply to Message

Serge E. Hallyn [serue@us.ibm.com] wrote:
| Quoting sukadev@us.ibm.com (sukadev@us.ibm.com):
| >
| > From: Sukadev Bhattiprolu <sukadev@us.ibm.com>
| > Subject: [PATCH 6/7]: Check for user-space mount of /dev/pts
| >
| > When the pts namespace is cloned, the /dev/pts is not useful unless it
| > is remounted from the user space.
| >
| > If user-space clones pts namespace but does not remount /dev/pts, it
| > would end up using the /dev/pts mount from parent-pts-ns but allocate
| > the pts indices from current pts ns.
|
| So why not use the allocated_ptys from the parent ptsns?  It's what
| userspace asked for and it's safe to do.

The problem is when opening /dev/ptmx, we use current_pts_ns() and
when opening slave-pty, we use pts_ns from the inode.

If child-pts-ns opens /dev/ptmx, we use 'allocated-ptys' from
child-pts-ns and we allocate index 0. But when the process opens
the slave pty "/dev/pts/0", we would get the pts_ns from the
inode which would come from parent-pts-ns (and could refer to
an existing pty).

Agree with Alexey and Pavel, its bad. Will think some more, but
appreciate any ideas.

Sukadev

_____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers