Subject: Re: [patch 7/9] unprivileged mounts: allow unprivileged fuse mounts
Posted by Pavel Machek on Wed, 09 Jan 2008 11:33:25 GMT
View Forum Message <> Reply to Message

Hi!

> > > AFAIR there were two security vulnerabilities in fuse's history, one
> > > of them an information leak in the kernel module, and the other one an
> > > mtab corruption issue in the fusermount utility. I don't think this
> > > is such a bad track record.
> >
> > Not bad indeed. But I'd consider 'kill -9 not working' to be DoS
> > vulnerability...
>
> The worst that can happen is that a sysadmin doesn't read the docs
> (likely) before enabling fuse on a multiuser system, and is surprised
> by a user doing funny things. And _then_ has to go read the docs, or
> google for some info. This is basically how things normally work, and
> I don't consider it a DoS.

No, this is not normal. Kill -9 has been estabilished long time ago,
and we should not be documenting its now-brokenness in
Documentation/filesystems/fuse.txt .

For example, my /etc/inittab currently has:

```
kb::kbrequest:/etc/rc/rc.reboot 2 0

#
# This file handles system shutdown and reboot.
#

PATH=/sbin:/bin:/usr/sbin:/usr/bin
sync &

# Kill all processes.
wall System is going down NOW\!
echo -n -e "\rSystem is going down: processes."
killall5 -15
echo -n "."
sleep 1
echo -n ". "
killall5 -9

# Before unmounting file systems write a reboot record to wtmp.
echo -n "wtmp "
halt -w
```

```
# Swap needs to be unmounted because otherwise busy filesystems
remain.
echo -n "swap "
swapoff -a
swapoff /c/swap
swapoff /c/swap2

# Unmount file systems
echo -n "umount."
umount -a || (
 sync &
 echo -n "umount-retry."
 sleep 1
 umount -a || sulogin
)
echo -n ". "
mount -n -o remount,ro /

# Now halt or reboot.
if [ "$2" = "0" ] ; then
 swapoff -a
 echo "halted."
 halt -p -f
else
 echo "rebooting..."
 reboot -d -f
fi
```

...this will break with FUSE enabled, right? (Minor security hole by allowing users to stop c-a-delete, where none existed before?)

I'm currently suspending by 'echo "mem" > /sys/power/state'. How should I do that _safely_ with FUSE enabled?

If I want to get rid of nasty user in multiuser system, I do su nastyuser 'kill -9 -1' . How do I do the equivalent with FUSE enabled? (Without affecting other users?)

Load average was never really meaningful number, but with FUSE enabled, users can set it to 666 without actually eating any CPU.

SIGSTOP used to work, allowing you to prevent user processes from working while you examine them. Now SIGSTOP can be delayed for arbitrary time.

Heck, imagine malicious user process misbehaves. Before FUSE, you could at least attach it with gdb to look what it is doing. Now you can't.

I really believe FUSE vs. signals needs fixing. Either that, or
updating all the manpages

man 1 kill:
- KILL 9 exit this signal may not be blocked
+ KILL 9 exit this signal may not be blocked, except by FUSE user mount

  Pavel
--
(english) http://www.livejournal.com/~pavelmachek
(cesky, pictures) http://atrey.karlin.mff.cuni.cz/~pavel/picture/horses/blog.html
_____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers