
Subject: Re: [PATCH] Masquerade sender information
Posted by [ebiederm](#) on Thu, 01 Nov 2007 16:59:31 GMT
[View Forum Message](#) <> [Reply to Message](#)

sukadev@us.ibm.com writes:

```
> +static void masquerade_sender(struct task_struct *t, struct sigqueue *q)
> +{
> +    /*
> +     * If the sender does not have a pid_t in the receiver's active
> +     * pid namespace, set si_pid to 0 and pretend signal originated
> +     * from the kernel.
> +     */
> +    if (!pid_ns_equal(t)) {
> +        q->info.si_pid = 0;
> +        q->info.si_uid = 0;
> +        q->info.si_code = SI_KERNEL;
> +    }
> +}
```

It looks like we are hooked in the right place. However the way we are handling this appears wrong.

First. If we have an si_code that does not use si_pid then we should not be changing si_pid, because the structure is a union and that field is not always a pid value.

My gut feel says the code should be something like:

```
switch (q->info->si_code & __SI_MASK) {
case __SI_KILL:
case __SI_CHILD:
case __SI_RT:
case __MESQ:
    q->info->si_pid = task_pid_nr_ns(current, t->nsproxy->pid_ns);
    break;
}
```

Eric

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