Subject: [PATCH][VLAN] Lost rtnl_unlock() in vlan_ioctl()
Posted by Pavel Emelianov on Thu, 06 Dec 2007 13:52:00 GMT
View Forum Message <> Reply to Message

The SET_VLAN_NAME_TYPE_CMD command w/o CAP_NET_ADMIN capability
doesn't release the rtnl lock.

Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

```
diff --git a/net/8021q/vlan.c b/net/8021q/vlan.c
index 6567213..5b18315 100644
--- a/net/8021q/vlan.c
+++ b/net/8021q/vlan.c
@@ -776,7 +776,7 @@ static int vlan_ioctl_handler(struct net *net, void __user *arg)
  case SET_VLAN_NAME_TYPE_CMD:
   err = -EPERM;
   if (!capable(CAP_NET_ADMIN))
-   return -EPERM;
+   break;
   if ((args.u.name_type >= 0) &&
       (args.u.name_type < VLAN_NAME_TYPE_HIGHEST)) {
    vlan_name_type = args.u.name_type;
```

Subject: Re: [PATCH][VLAN] Lost rtnl_unlock() in vlan_ioctl()
Posted by Patrick McHardy on Thu, 06 Dec 2007 13:59:24 GMT
View Forum Message <> Reply to Message

Pavel Emelyanov wrote:
> The SET_VLAN_NAME_TYPE_CMD command w/o CAP_NET_ADMIN capability
> doesn't release the rtnl lock.

Thanks Pavel. I somehow recall that we already fixed this
one, but can't find the patch :) Dave, please apply.

Subject: Re: [PATCH][VLAN] Lost rtnl_unlock() in vlan_ioctl()
Posted by davem on Thu, 06 Dec 2007 14:01:51 GMT
View Forum Message <> Reply to Message

From: Patrick McHardy <kaber@trash.net>
Date: Thu, 06 Dec 2007 14:59:24 +0100

> Pavel Emelyanov wrote:

> > The SET_VLAN_NAME_TYPE_CMD command w/o CAP_NET_ADMIN capability
> > doesn't release the rtnl lock.
>
>
> Thanks Pavel. I somehow recall that we already fixed this
> one, but can't find the patch :) Dave, please apply.

I think we even added this bug to -stable, or something like
that, didn't we? Yikes...

Subject: Re: [PATCH][VLAN] Lost rtnl_unlock() in vlan_ioctl()
Posted by Patrick McHardy on Thu, 06 Dec 2007 14:10:35 GMT
View Forum Message <> Reply to Message

David Miller wrote:
> From: Patrick McHardy <kaber@trash.net>
> Date: Thu, 06 Dec 2007 14:59:24 +0100
>
>> Pavel Emelyanov wrote:
>>> The SET_VLAN_NAME_TYPE_CMD command w/o CAP_NET_ADMIN capability
>>> doesn't release the rtnl lock.
>>
>> Thanks Pavel. I somehow recall that we already fixed this
>> one, but can't find the patch :) Dave, please apply.
>
> I think we even added this bug to -stable, or something like
> that, didn't we? Yikes...

No, I mixed those two patches up as well. The bug was introduced
with the vlan_netlink stuff, the -stable patch fixed an invalid
return value, but still properly dropped the lock.

This patch should of course go in -stable anyway.

Subject: Re: [PATCH][VLAN] Lost rtnl_unlock() in vlan_ioctl()
Posted by davem on Fri, 07 Dec 2007 06:52:55 GMT
View Forum Message <> Reply to Message

From: Patrick McHardy <kaber@trash.net>
Date: Thu, 06 Dec 2007 14:59:24 +0100

> Pavel Emelyanov wrote:
> > The SET_VLAN_NAME_TYPE_CMD command w/o CAP_NET_ADMIN capability
> > doesn't release the rtnl lock.

>
>
> Thanks Pavel. I somehow recall that we already fixed this
> one, but can't find the patch :) Dave, please apply.

Applied and I'll push to -stable once Linus pulls it in.
