# Subject: Re: [PATCH][NEIGH] Fix race between neigh_parms_release and neightbl_fill_parms

Posted by davem on Thu, 10 Jan 2008 11:50:32 GMT

View Forum Message <> Reply to Message

From: Pavel Emelyanov <xemul@openvz.org>
Date: Thu, 10 Jan 2008 13:56:53 +0300

> The neightbl_fill_parms() is called under the write-locked
> tbl->lock and accesses the parms->dev. The negh_parm_release()
> calls the dev_put(parms->dev) without this lock. This
> creates a tiny race window on which the parms contains
> potentially stale dev pointer.
>
> To fix this race it's enough to move the dev_put() upper
> under the tbl->lock, but note, that the parms are held by
> neighbors and thus can live after the neigh_parms_release()
> is called, so we still can have a parm with bad dev pointer.
>
> I didn't find where the neigh->parms->dev is accessed, but
> still think that putting the dev is to be done in a place,
> where the parms are really freed. Am I right with that?
>
> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

It is accessed in lookup_neigh_parms(), neightbl_fill_parms(), and neightbl_fill_info() (hmmm, that BUG_ON(tbl->parms.dev) is cute).

You fix looks correct, patch applied, thanks!