

---

Subject: Re: [PATCH 2/3] Lost locking in fl6\_sock\_lookup

Posted by [yoshfuji](#) on Thu, 18 Oct 2007 12:00:43 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

In article <47174950.6060409@openvz.org> (at Thu, 18 Oct 2007 15:53:52 +0400), Pavel Emelyanov <xemul@openvz.org> says:

> This routine scans the ipv6\_fl\_list whose update is  
> protected with the socket lock and the ip6\_sk\_fl\_lock.

```
> struct ip6_flowlabel *fl = sfl->fl;  
> if (fl->label == label) {  
> + read_unlock_bh(&ip6_sk_fl_lock);  
> fl->lastuse = jiffies;  
> atomic_inc(&fl->users);  
> return fl;
```

We should increment fl->users within the critical section, shouldn't we?

--yoshfuji

---