Subject: [PATCH 2/3] Lost locking in fl6_sock_lookup
Posted by Pavel Emelianov on Thu, 18 Oct 2007 11:53:52 GMT
View Forum Message <> Reply to Message

This routine scans the ipv6_fl_list whose update is
protected with the socket lock and the ip6_sk_fl_lock.

Since the socket lock is not taken in the lookup, use
the other one.

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

```
diff --git a/net/ipv6/ip6_flowlabel.c b/net/ipv6/ip6_flowlabel.c
index 8550df2..f40a086 100644
--- a/net/ipv6/ip6_flowlabel.c
+++ b/net/ipv6/ip6_flowlabel.c
@@ -190,14 +190,17 @@ struct ip6_flowlabel * fl6_sock_lookup(struct sock *sk, __be32 label)

  label &= IPV6_FLOWLABEL_MASK;

+ read_lock_bh(&ip6_sk_fl_lock);
  for (sfl=np->ipv6_fl_list; sfl; sfl = sfl->next) {
   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;
   }
  }
+ read_unlock_bh(&ip6_sk_fl_lock);
  return NULL;
 }
```