Subject: [PATCH][IPV6]: Mischecked tw match in __inet6_check_established.
Posted by Pavel Emelianov on Tue, 15 Jan 2008 09:22:52 GMT
View Forum Message <> Reply to Message

When looking for a conflicting connection the !sk->sk_bound_dev_if
check is performed only for live sockets, but not for timewait-ed.

This is not the case for ipv4, for __inet6_lookup_established in
both ipv4 and ipv6 and for other places that check for tw-s.

Was this missed accidentally? If so, then this patch fixes it and
besides makes use if the dif variable declared in the function.

Fits both, net-2.6 and net-2.6.25.

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

```
diff --git a/net/ipv6/inet6_hashtables.c b/net/ipv6/inet6_hashtables.c
index d0b3447..a66a7d8 100644
--- a/net/ipv6/inet6_hashtables.c
+++ b/net/ipv6/inet6_hashtables.c
@@ -193,7 +193,7 @@ static int __inet6_check_established(struct inet_timewait_death_row
*death_row,
      sk2->sk_family        == PF_INET6  &&
      ipv6_addr_equal(&tw6->tw_v6_daddr, saddr)  &&
      ipv6_addr_equal(&tw6->tw_v6_rcv_saddr, daddr) &&
-     sk2->sk_bound_dev_if == sk->sk_bound_dev_if) {
+     (!sk2->sk_bound_dev_if || sk2->sk_bound_dev_if == dif)) {
    if (twsk_unique(sk, sk2, twp))
     goto unique;
    else
```

Subject: Re: [PATCH][IPV6]: Mischecked tw match in __inet6_check_established.
Posted by davem on Tue, 15 Jan 2008 11:33:43 GMT
View Forum Message <> Reply to Message

From: Pavel Emelyanov <xemul@openvz.org>
Date: Tue, 15 Jan 2008 12:22:52 +0300

> When looking for a conflicting connection the !sk->sk_bound_dev_if
> check is performed only for live sockets, but not for timewait-ed.
>
> This is not the case for ipv4, for __inet6_lookup_established in
> both ipv4 and ipv6 and for other places that check for tw-s.
>

> Was this missed accidentally? If so, then this patch fixes it and
> besides makes use if the dif variable declared in the function.
>
> Fits both, net-2.6 and net-2.6.25.
>
> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

This fix definitely looks correct.

I just sent Linus a pull request for other 2.6.24 fixes,
so I'll toss this into my net-2.6 tree tomorrow after
he pulls that stuff in.

Thanks!
