Subject: Re: [PATCH (resubmit)] Fix inet_diag.ko register vs rcv race
Posted by Pavel Emelianov on Mon, 03 Dec 2007 09:01:06 GMT
View Forum Message <> Reply to Message

Herbert Xu wrote:
> On Thu, Nov 29, 2007 at 04:01:25PM +0300, Pavel Emelyanov wrote:
>> @@ -863,13 +861,13 @@ int inet_diag_register(const struct inet_diag_handler *h)
>> if (type >= INET_DIAG_GETSOCK_MAX)
>> goto out;
>>
>> - spin_lock(&inet_diag_register_lock);
>> + mutex_lock(&inet_diag_mutex);
>> err = -EEXIST;
>> if (inet_diag_table[type] == NULL) {
>> inet_diag_table[type] = h;
>> err = 0;
>> }
>> - spin_unlock(&inet_diag_register_lock);
>> + mutex_unlock(&inet_diag_mutex);
>
> Actually this causes a dead-lock when the handlers are built as modules
> because we try to load them with that mutex held.

Ouch! Sorry, I didn't notice this :(

> I've fixed it with this patch on top.

Thanks!

> Cheers,

Pavel