

---

Subject: Re: [NETLINK] Don't attach callback to a going-away netlink socket  
Posted by [xemul](#) on Wed, 18 Apr 2007 08:27:56 GMT

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

---

Evgeniy Polyakov wrote:

> On Wed, Apr 18, 2007 at 12:16:18PM +0400, Pavel Emelianov (xemul@sw.ru) wrote:

>> Sorry, I forgot to put netdev and David in Cc when I first sent it.

>>

>> There is a race between netlink\_dump\_start() and netlink\_release()

>> that can lead to the situation when a netlink socket with non-zero

>> callback is freed.

>

> Out of curiosity, why not to fix a netlink\_dump\_start() to remove

> callback in error path, since in 'no-error' path it removes it in

Error path is not relevant here. The problem is that we  
keep a callback on a socket that is about to be freed.

> netlink\_dump().

>

> And, btw, can release method be called while socket is being used, I

> thought about proper reference counters should prevent this, but not

> 100% sure with RCU dereferencing of the descriptor.

>

---