
Subject: Re: [PATCH] [RFC] nfsd: fix possible dereference of static NULL nfsd_serv pointer

Posted by [bfields](#) on Tue, 10 Jul 2012 15:59:43 GMT

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

On Sat, Jul 07, 2012 at 09:27:30AM +0400, Stanislav Kinsbursky wrote:

> >On Fri, Jul 06, 2012 at 05:45:56PM +0400, Stanislav Kinsbursky wrote:

> >>This is a bug fix for 3.5 kernel.

> >>In case on NFSd service start failure svc_shutdown_net() will call svc_destroy

> >>callback and zeroize global nfsd_serv pointer, this in turn will lead to Oops

> >>in svc_destroy().

> >>

> >>This patch is marked as RFC, because to many lines were changed. It can be

> >>easily simplified if requested.

> >>Moreover, NFSd service shutdown is going to be converted into something on

> >>per-net basis.

> >Doesn't this leave error paths in e.g. __write_ports_addfd() and

> >__write_ports_addxprt() unfixed?

>

> Yes, sure it does...

>

> >I'm inclined to just submit your original fix (split up as in the last

> >version I sent) for 3.5 if you don't object.

>

> Not at all.

> Thanks, Bruce.

OK. Actually, Linus is making noise about a release in the next week or two, so given that this is about error paths, I'm going to queue it up for the 3.6 and cc it to stable. It'll end up in 3.5.x pretty quickly that way anyway.

--b.
