Subject: Re: [PATCH] remove BUG() in possible but rare condition
Posted by Michal Hocko on Wed, 11 Apr 2012 19:25:54 GMT
View Forum Message <> Reply to Message

On Wed 11-04-12 16:02:19, Glauber Costa wrote:
> On 04/11/2012 03:57 PM, Linus Torvalds wrote:
> >On Wed, Apr 11, 2012 at 11:48 AM, Michal Hocko<mhocko@suse.cz> wrote:
> >>
> >>I am not familiar with the code much but a trivial call chain walk up to
> >>write_dev_supers (in btrfs) shows that we do not check for the return value
> >>from __getblk so we would nullptr and there might be more.
> >>I guess these need some treat before the BUG might be removed, right?
> >
> >Well, realistically, isn't BUG() as bad as a NULL pointer dereference?
> >
> >Do you care about the exact message on the screen when your machine dies?
> Not particular, but I don't see why (I might be wrong) it would
> necessarily lead to a NULL pointer dereference.

Ahh, OK scratch that. I have misread __getblk_slow which returns NULL
only if grow_buffers returned with < 0 which doesn't happen for the
allocation failure.

Sorry about noise
--
Michal Hocko
SUSE Labs
SUSE LINUX s.r.o.
Lihovarska 1060/12
190 00 Praha 9
Czech Republic