Subject: Re: [PATCH RESEND 2/2] Fix some kallsyms_lookup() vs rmmod races
Posted by Rusty Russell on Sat, 17 Mar 2007 09:32:51 GMT
View Forum Message <> Reply to Message

On Fri, 2007-03-16 at 14:44 +0300, Alexey Dobriyan wrote:
> [cc'ing folks whose proc files are affected]
>
> kallsyms_lookup() can call module_address_lookup() which iterates over
> modules list without module_mutex taken. Comment at the top of
> module_address_lookup() says it's for oops resolution so races are
> irrelevant, but in some cases it's reachable from regular code:

Yes, this changed somewhere along the way.

I prefer keeping the lock internal as much as possible, and have the
crash code use an __ variant of the function.

Note also that it might be an idea to have less-powerful accessors than
kallsyms_lookup...

Thanks!
Rusty.