Subject: Re: [PATCH RESEND 2/2] Fix some kallsyms_lookup() vs rmmod races Posted by Rusty Russell on Sat, 17 Mar 2007 09:37:18 GMT

View Forum Message <> Reply to Message

On Fri, 2007-03-16 at 12:51 +0100, Ingo Molnar wrote:

- > * Alexey Dobriyan <adobriyan@sw.ru> 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:

>

- > looking at the problem from another angle: wouldnt this be something
- > that would benefit from freeze_processes()/unfreeze_processes(), and
- > hence no locking would be required?

Actually, the list manipulation is done with stop_machine for this reason. Alexey, is preempt enabled in your kernel?

Rusty.