Subject: Re: [PATCH] Fix some kallsyms_lookup() vs rmmod races
Posted by Paulo Marques on Thu, 15 Mar 2007 16:53:59 GMT
View Forum Message <> Reply to Message

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:

So maybe we should just add a new parameter to "kallsyms_lookup" to
inform it if it is safe to take a mutex or not.

Spreading module_mutex everywhere doesn't seem like the right interface
for several reasons:

  - new users of "kallsyms_lookup" might not be aware that they should
take module_mutex if it is safe

  - many times we will be taking module_mutex even when we are fetching
a kernel symbol that shouldn't require the mutex at all

  - it just creates new dependencies (hint: this patch shouldn't even
compile with current git since module_mutex is not declared in module.h,
not to mention compile when CONFIG_MODULES not set)

IMHO we should not expose module_mutex outside of module.c. That is just
wrong from an encapsulation point of view.

--
Paulo Marques - www.grupopie.com

"667: The neighbor of the beast."