
Subject: Re: [PATCH v3] Race between cat /proc/kallsyms and rmmod

Posted by [Rusty Russell](#) on Mon, 19 Mar 2007 23:35:11 GMT

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

On Mon, 2007-03-19 at 17:33 +0300, Alexey Dobriyan wrote:

> Iterating code of /proc/kallsyms calls module_get_kallsym() which grabs
> and drops module_mutex internally and returns "struct module *",
> module is removed, aforementioned "struct module *" is used in non-trivial
> way.

Hi Alexey,

I like the patch, but I wonder if passing the lengths for the symbol and module name is overkill? There are KSYM_NAME_LEN and MODULE_NAME_LEN constants, after all, and we could just have the callers use buffers of sufficient size. Simplifies the code and reduces confusion if someone passes a small buffer and it gets surprisingly truncated...

Thanks!

Rusty.
