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

Posted by [Paulo Marques](#) on Mon, 19 Mar 2007 15:20:43 GMT

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

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.

>

> Steps to reproduce:

>

> modprobe/rmmod loop

> cat /proc/kallsyms >/dev/null loop

>

> Copy all needed info under module_mutex.

>

> NOTE: this patch keeps module_mutex static.

Yes, this patch fixes the "cat /proc/kallsyms" race without changing any
"external" interfaces, so I think it should go into mainline in any case.

Acked-by: Paulo Marques <pmarques@grupopie.com>

--

Paulo Marques - www.grupopie.com

"All I ask is a chance to prove that money can't make me happy."
