## Subject: [PATCH] Fix leak on /proc/lockdep_stats
Posted by Alexey Dobriyan on Tue, 17 Jul 2007 12:57:36 GMT

View Forum Message <> Reply to Message

On Tue, Jul 17, 2007 at 02:36:10PM +0200, Ingo Molnar wrote:
> * Alexey Dobriyan <adobriyan@sw.ru> wrote:
>
> > On every open/close one struct seq_operations leaks.
> > Kudos to /proc/slab_allocators.
> >
> > Signed-off-by: Alexey Dobriyan <adobriyan@sw.ru>
>
> ouch ...
>
> Acked-by: Ingo Molnar <mingo@elte.hu>
>
> -stable material too, as far as timer_info/stats goes.
>
> > -        .release        = seq_release,
> > +        .release        = single_release,
>
> i think seq_release() definitely needs to grow a WARN_ON() if it's being
> used on an inode that was opened via single_open(). This bug is so
> easily committed, and nothing but a small leak reminds us on it.

Yeah, I'll try to come up with something clean.

Meanwhile full single_open() audit revealed one more such leak.
The rest seems OK.

[PATCH] Fix leak on /proc/lockdep_stats

Signed-off-by: Alexey Dobriyan <adobriyan@sw.ru>
---

 kernel/lockdep_proc.c |    2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)

--- a/kernel/lockdep_proc.c
+++ b/kernel/lockdep_proc.c
@@ -339,7 +339,7 @@ static const struct file_operations proc_lockdep_stats_operations = {
  .open  = lockdep_stats_open,
  .read  = seq_read,
  .llseek  = seq_lseek,
- .release = seq_release,
+ .release = single_release,
 };

static int __init lockdep_proc_init(void)