Subject: Re: [SCSI] 3w-9xxx: kmap_atomic in twa_scsiop_execute_scsi
Posted by Adam Radford on Tue, 06 Jun 2006 18:46:56 GMT
View Forum Message <> Reply to Message

Vasily,

On 6/5/06, Vasily Averin <vvs@sw.ru> wrote:

> I'm agree that queuecommand() executed with disabled interrupts. However
> twa_scsiop_execute_scsi() can be called not only from queuecommand. For example,
>
> twa_interrupts (note: with _enabled_ interrupts)
> twa_aen_read_queue
> twa_scsiop_execute_scsi
>

twa_scsiop_execute_scsi() will not perform the kmap_atomic()/kunmap_atomic()
calls here because it is being used for an internal AEN drain (cdb
post), i.e. "sglistarg" is non NULL. See below:

```
if (!sglistarg) {

  ....
   kmap_atomc()
   kunmap_atomic()

} else {
   /* Internal cdb post */

}
```

> or
>
> twa_chrdev_ioctl
> twa_reset_device_extension
> twa_reset_sequence
> twa_aen_drain_queue
> twa_scsiop_execute_scsi

ditto for this location as well.

Thanks for looking over this code. If you see anything else suspect,
feel free to let me know.

-Adam

>
> Thank you,

> Vasily Averin
>
> SWsoft Virtuozzo/OpenVZ Linux kernel team
>
> > -----Original Message-----
> > From: Vasily Averin [mailto:vvs@sw.ru]
> > Sent: Sunday, June 04, 2006 1:49 AM
> > To: adam radford; linuxraid
> > Cc: James Bottomley; Linux Kernel Mailing List;
> > linux-scsi@vger.kernel.org; devel@openvz.org; Andrew Morton
> > Subject: [SCSI] 3w-9xxx: kmap_atomic in twa_scsiop_execute_scsi
> >
> > Hello Adam,
> >
> > you have fixed recently potential memory corruption, kmap_atomic issue
> > in 3w-9xxx driver, however it seems for me you have forgotten to fix the
> > same issue in yet another similar place, in twa_scsiop_execute_scsi()
> > function.
> >
> > Signed-off-by: Vasily Averin <vvs@sw.ru>
> >
> > Thank you,
> > Vasily Averin
> >
> > SWsoft Virtuozzo/OpenVZ Linux kernel team
> >
> >
>
>