Subject: Re: [SCSI] 3w-9xxx: kmap_atomic in twa_scsiop_execute_scsi
Posted by vaverin on Tue, 06 Jun 2006 05:46:29 GMT

View Forum Message <> Reply to Message

Adam Radford wrote:
> Vasily,
>
> I actually didn't forget this. I think it isn't needed. The reason
> being
> that in scsi.c: scsi_dispatch_command(), where hostt->queuecommand() is
> called,
> there is a spin_lock_irqsave()/spin_unlock_irqrestore() wrapper in
> there, disabling
> interrupts.

Adam,

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
```

or

```
twa_chrdev_ioctl
   twa_reset_device_extension
      twa_reset_sequence
         twa_aen_drain_queue
            twa_scsiop_execute_scsi
```

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
>
>