Subject: [SCSI] 3w-9xxx: kmap_atomic in twa_scsiop_execute_scsi
Posted by vaverin on Sun, 04 Jun 2006 08:46:35 GMT
View Forum Message <> Reply to Message

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

```
--- a/drivers/scsi/3w-9xxx.c 2006-06-04 11:15:52.000000000 +0400
+++ b/drivers/scsi/3w-9xxx.c 2006-06-04 11:18:34.000000000 +0400
@@ -1864,9 +1864,13 @@ static int twa_scsiop_execute_scsi(TW_De
   if ((tw_dev->srb[request_id]->use_sg == 1) && (tw_dev->srb[request_id]->request_bufflen <
TW_MIN_SGL_LENGTH)) {
    if (tw_dev->srb[request_id]->sc_data_direction == DMA_TO_DEVICE ||
tw_dev->srb[request_id]->sc_data_direction == DMA_BIDIRECTIONAL) {
     struct scatterlist *sg = (struct scatterlist *)tw_dev->srb[request_id]->request_buffer;
-     char *buf = kmap_atomic(sg->page, KM_IRQ0) + sg->offset;
+     unsigned long flags = 0;
+     char *buf;
+     local_irq_save(flags);
+     buf = kmap_atomic(sg->page, KM_IRQ0) + sg->offset;
     memcpy(tw_dev->generic_buffer_virt[request_id], buf, sg->length);
     kunmap_atomic(buf - sg->offset, KM_IRQ0);
+     local_irq_restore(flags);
    }
    command_packet->sg_list[0].address =
TW_CPU_TO_SGL(tw_dev->generic_buffer_phys[request_id]);
    command_packet->sg_list[0].length = cpu_to_le32(TW_MIN_SGL_LENGTH);
```

Subject: RE: [SCSI] 3w-9xxx: kmap_atomic in twa_scsiop_execute_scsi
Posted by Adam Radford on Mon, 05 Jun 2006 18:23:08 GMT
View Forum Message <> Reply to Message

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

-----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

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
>
>

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
> >
> >
>
>

Subject: Re: [SCSI] 3w-9xxx: kmap_atomic in twa_scsiop_execute_scsi
Posted by vaverin on Tue, 06 Jun 2006 19:25:25 GMT
View Forum Message <> Reply to Message

Adam,

adam radford wrote:
> 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 */
>
> }
```

Ok, I'm agree.

Thank you for your explanation,
 Vasily Averin

SWsoft Virtuozzo/OpenVZ Linux kernel team