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);
```