

patch: fix ata panic with Thinkpad CD and DVD drives

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2005-02/1165.html>

From: Nate Lawson (nate_at_root.org)

Date: 02/27/05

Date: Sun, 27 Feb 2005 11:56:06 -0800

To: current@freebsd.org

If you've been having "memory modified after free" panics on -current and have a Thinkpad, the attached patch should fix things for you. A quick check of RELENG_5 indicates that the bug is probably there also but I haven't tested for it there.

The bug is triggered by timeouts in the ata_getparam() probe path. The ata_timeout() fires and ata_end_transaction() is called to get the status. However, it continues down into ata_pio_read() even though there is no data available since we had a timeout, not read completion.

ata_pio_read() reads 512 bytes of probably bogus data. The important problem is that it also advances donecount. On subsequent timeouts (note there are 4 below), donecount advances into unallocated memory and so subsequent ata_pio_read() calls overwrite 512 bytes of someone else's memory.

The fix is to exit immediately if ATA_R_TIMEOUT is set after reading the status in ata_end_transaction(). It shouldn't go into ata_pio_read() if there was a timeout. The patch does this.

However, it only handles PIO timeouts since I wasn't sure the best way to proceed for unwinding DMA state and the like for the other cases. This is enough to fix the overwrite and subsequent panic on my systems.

I've run heavy IO stress and DVD accesses for a while and no further panics.

While looking into this, I found another potential problem. In one reinjection case, donecount wasn't reset to 0. The patch for ata-queue.c does this and I think it's necessary but don't hit this case in testing so I can't be sure. Finally, there's one whitespace nit that helps with clarity.

These are similar bugs to one found back in August that had the same effect. Here's the closest reference I could find in the mail archives for this:

<http://lists.freebsd.org/mailman/htdig/freebsd-current/2004-August/033033.html>

freebsd-current: patch: fix ata panic with Thinkpad CD and DVD drives

Please fix this before 5.4-R, thanks.

Here is the hardware in question. This bug is triggered by various CD, DVD, CDRW, etc. drives shipped with Thinkpads.

```
atapci0: <Intel ICH3 UDMA100 controller> port
0x1860-0x186f,0x376,0x170-0x177,0x3f6,0x1f0-0x1f7 at device 31.1 on pci0
ata0: channel #0 on atapci0
ata1: channel #1 on atapci0

ad0: 19077MB <IC25N020ATMR04-0/MO1OAD4A> [41344/15/63] at ata0-master
UDMA100
ata1-slave: FAILURE - ATAPI_IDENTIFY timed out
ata1-slave: FAILURE - ATAPI_IDENTIFY timed out
ata1-slave: FAILURE - ATAPI_IDENTIFY timed out
ata1-slave: FAILURE - ATAPI_IDENTIFY timed out
acd0: FAILURE - SETFEATURES SET TRANSFER MODE timed out
acd0: DVDROM <HL-DT-STDVD-ROM GDR8081N/0012> at ata1-master UDMA33
```

--
Nate

Index: sys/dev/ata/ata-lowlevel.c

```
=====
RCS file: /home/ncvs/src/sys/dev/ata/ata-lowlevel.c,v
retrieving revision 1.51
diff -u -r1.51 ata-lowlevel.c
--- sys/dev/ata/ata-lowlevel.c 24 Dec 2004 13:38:25 -0000 1.51
+++ sys/dev/ata/ata-lowlevel.c 27 Feb 2005 19:23:09 -0000
@@ -297,6 +297,9 @@
```

```
    /* ATA PIO data transfer and control commands */
    default:
+ /* XXX Doesn't handle the non-PIO case. */
+ if (request->flags & ATA_R_TIMEOUT)
+ return ATA_OP_FINISHED;

    /* on control commands read back registers to the request struct */
    if (request->flags & ATA_R_CONTROL) {
@@ -321,7 +324,7 @@
        ata_pio_read(request, request->transfersize);

    /* update how far we've gotten */
- request->donecount += request->transfersize;
+ request->donecount += request->transfersize;

    /* do we need a scoop more ? */
    if (request->bytecount > request->donecount) {
```

Index: sys/dev/ata/ata-queue.c

freebsd-current: patch: fix ata panic with Thinkpad CD and DVD drives

```
RCS file: /home/ncvs/src/sys/dev/ata/ata-queue.c,v
retrieving revision 1.41
diff -u -r1.41 ata-queue.c
--- sys/dev/ata/ata-queue.c 8 Dec 2004 11:16:33 -0000 1.41
+++ sys/dev/ata/ata-queue.c 27 Feb 2005 19:22:16 -0000
@@ -249,6 +249,7 @@
     && request->device->param){
     request->flags &= ~(ATA_R_TIMEOUT | ATA_R_DEBUG);
     request->flags |= (ATA_R_IMMEDIATE | ATA_R_QUEUE);
+ request->donecount = 0;
     ATA_DEBUG_RQ(request, "completed reinject");
     ata_queue_request(request);
     return;
```

freebsd-current@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-current>

To unsubscribe, send any mail to "freebsd-current-unsubscribe@freebsd.org"