

BTX loader reboot on Soekris comBIOS1.22 fails (patches for btx.s and loader/main.c enclosed)

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2003-11/0205.html>

From: Adrian Steinmann (*ast_at_marabu.ch*)

Date: 11/16/03

Date: Sun, 16 Nov 2003 02:31:31 +0100
To: Soren Kristensen <soren@soekris.com>

After "reboot" in the FreeBSD-stable BTX loader just hangs on Soekris comBIOS 1.22 Soren asked me:
... how does the loader do the actual
reboot ? And does it differ from how FreeBSD otherwise reboots ?

I have investigated this now: from FreeBSD, /sbin/reboot first tries a 8042 keyboard reset, i.e. it writes 0xFE to 0x064.

On FreeBSD-stable this is near line 441 in /usr/src/sys/i386/i386/vm_machdep.c (unless a kernel config BROKEN_KEYBOARD_RESET is defined):

```
#if !defined(BROKEN_KEYBOARD_RESET)
    outb(IO_KBD + 4, 0xFE);
    DELAY(500000); /* wait 0.5 sec to see if that did it */
    printf("Keyboard reset did not work, attempting CPU shutdown\n");
    DELAY(1000000); /* wait 1 sec for printf to complete */
#endif
```

this works on Soekris comBIOS 1.22.

If the above fails, vm_machdep.ch falls back to unmapping the address space and invalidating TLD:

```
/* force a shutdown by unmapping entire address space ! */
bzero((caddr_t) PTD, PAGE_SIZE);

/* "good night, sweet prince .... <THUNK!>" */
invltlb();
```

but since the keyboard reset works work, this case is never used (on Soekris) on /sbin/reboot.

In the BTX loader, the reboot command simply exits the loader, and end up in exit near line 252 in /usr/src/sys/boot/i386/btx/btx/btx.s which disables paging, flushes TLB, switches to real mode, flags a

freebsd-hackers: BTX loader reboot on Soekris comBIOS1.22 fails (patches for btx.s and loader/main.c enclosed)

warm boot (writes 0x1234 to 0x472) and then jumps to the BIOS reboot handler:

```
- ljmp $0xffff,$0x0 # reboot the machine
```

however in various literature it is mentioned that \$0xf000,\$0xffff is bound to work better on most platforms, so I tried

```
+ ljmp $0xf000,$0xffff # reboot the machine
```

which indeed works! (OpenBSD, for example, uses ljmp \$0xf000,\$0xffff).

I prefer the KEYBOARD_RESET method because it follows the /sbin/reboot style, but I think FreeBSD should consider using ljmp \$0xf000,\$0xffff instead of ljmp \$0xffff,\$0x0 in btx.s for better compatibility.

For this reason I'm copying msmith@ and jhb@ and hackers@

I hope you can confirm that Soekris comBIOS 1.22 acts strangely when ljmp \$0xffff,\$0x0 is used.

The choice \$0xffff,\$0x0 was made Feb 2000 by jhb and msmith and was committed to version btx.s 1.15 with these comments:

- 1) Fix a bug in the int15 function 87 emulation where we only copied half of what the BIOS asked for. This caused the Mylex RAID adapter to go haywire and start trashing memory when you tried to boot from it.
- 2) Don't use interrupt 19 to reboot. Instead, set the reboot flag to a warm boot and jump to the BIOS's reboot handler. int 19 doesn't clear memory or restore the interrupt vector table, and thus really isn't safe. For example, when booting off of PXE, the PXE BIOS eats up a chunk of memory for its internal data and structures. Since we rebooted via int 19, using the 'reboot' command in the loader resulted in that memory not being reclaimed by the BIOS. Thus, after a few PXE boots, the system was out of lower memory.
- 3) Catch any int 19 calls made by a BTX client or a user pressing Ctrl-Alt-Delete and shutdown BTX and reboot the machine cleanly. This fixes Ctrl-Alt-Delete in the loader and in boot2 instead of presenting the user with a BTX fault.

These are the patches I have been using successfully (only one is necessary):

Index: usr/src/sys/boot/i386/btx/btx/btx.s

```
=====
RCS file: /usr/cvs/src/sys/boot/i386/btx/btx/btx.s,v
retrieving revision 1.15.2.4
diff -u -r1.15.2.4 btx.s
--- usr/src/sys/boot/i386/btx/btx/btx.s 28 Dec 2000 12:08:22 -0000 1.15.2.4
+++ usr/src/sys/boot/i386/btx/btx/btx.s 16 Nov 2003 00:26:28 -0000
@@ -293,7 +293,7 @@
     testb $0x1,btx_hdr+0x7 # Reboot?
     exit.3: jz exit.3 # No
             movw $0x1234, BDA_BOOT # Do a warm boot
- ljmp $0xffff,$0x0 # reboot the machine
```

BTX loader reboot on Soekris comBIOS1.22 fails (patches for btx.s and loader/main.c enclosed) 2

freebsd-hackers: BTX loader reboot on Soekris comBIOS1.22 fails (patches for btx.s and loader/main.c enclosed)

```
+ ljmp $0xf000,$0xffff # reboot the machine
#
# Set IRQ offsets by reprogramming 8259A PICs.
#
Index: usr/src/sys/boot/i386/loader/main.c
```

```
RCS file: /usr/cvs/src/sys/boot/i386/loader/main.c,v
retrieving revision 1.17.2.7
diff -u -r1.17.2.7 main.c
--- usr/src/sys/boot/i386/loader/main.c 10 Oct 2002 15:53:27 -0000 1.17.2.7
+++ usr/src/sys/boot/i386/loader/main.c 16 Nov 2003 00:26:28 -0000
@@ -35,6 +35,7 @@
#include <string.h>
#include <machine/bootinfo.h>
#include <sys/reboot.h>
+#include <i386/isa/isa.h>

#include "bootstrap.h"
#include "libi386/libi386.h"
@@ -238,6 +239,13 @@
    (devsw[i]->dv_cleanup());

    printf("Rebooting...\n");
+
+#if !defined(BROKEN_KEYBOARD_RESET)
+ isa_outb(IO_KBD + 4, 0xFE);
+ delay(1000000);
+ printf("Keyboard reset failed; exiting...\n");
+#endif
+
+    delay(1000000);
+    __exit(0);
}
```

freebsd-hackers@freebsd.org mailing list

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

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