

Linux-Kernel: qla2xxx: frequent total lockups (2.6.8, 2.6.9-rc{1-mm5,2})

qla2xxx: frequent total lockups (2.6.8, 2.6.9-rc{1-mm5,2})

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2004-09/5281.html>

From: Oliver M. Bolzer (*oliver_at_fakeroot.net*)

Date: 09/16/04

Date: Thu, 16 Sep 2004 01:16:59 +0200

To: linux-kernel@vger.kernel.org

Hi!

I'm currently setting up a new Dual Opteron box (Tyan Transport GX28) equipped with a QLogic QLA2340 fibre channel HBA.

As soon as there is I/O load on the HBA, I start seeing

```
qla2300 0000:01:03.0: qla2xxx_eh_abort: cmd already done sp=0000000000000000
```

messages every few seconds, eventually leading to complete system lockups after several minutes up to several hours, due to kernel NULL pointer dereferences in qla2x00_cmd_timeout().

I've tested and reproduced the error on the following kernels, all compiled for x86_64.

2.6.8.1

2.6.9-rc1-mm5 (with dma_fixups patch posted by Andrew Vasquez on 13.9)

2.6.9-rc2

Attached are a complete 2.6.9-rc1-mm5 log from boot to crash as well as two 2.6.9-rc2 crash dumps with only the post-boot messages.

The .config used and the complete logs can be found at <http://www.cip.ifi.lmu.de/~bolzer/tmp/qla-problem/>

Without any I/O on the HBA (nothing mounted), I have yet to capture a crash, but the driver still occasionally reports

```
qla2300 0000:01:03.0: cmd_timeout: LOST command state = 0x6
```

Any help would be greatly appreciated. If there are any tests I could run, just let me know.

```
Bootdata ok (command line is root=/dev/sda3 ro console=ttyS0,115200n8 console=tty0 )
Linux version 2.6.9-rc1-mm5 (root@bruellwuerfel) (gcc version 3.3.4 (Debian
1:3.3.4-6sarge1.2.0.1.pure64)) #8 SMP Wed Sep 15 13:14:15 CEST 2004
```

qla2xxx: frequent total lockups (2.6.8, 2.6.9-rc{1-mm5,2})

Linux-Kernel: qia2xxx: frequent total lockups (2.6.8, 2.6.9-rc{1-mm5,2})

BIOS-provided physical RAM map:

BIOS-e820: 0000000000000000 – 000000000009fc00 (usable)
BIOS-e820: 000000000009fc00 – 00000000000a0000 (reserved)
BIOS-e820: 00000000000e0000 – 0000000000100000 (reserved)
BIOS-e820: 0000000000100000 – 000000007fff0000 (usable)
BIOS-e820: 000000007fff0000 – 000000007ffff000 (ACPI data)
BIOS-e820: 000000007ffff000 – 0000000080000000 (ACPI NVS)
BIOS-e820: 00000000ff780000 – 0000000100000000 (reserved)

No mptable found.

ACPI: LAPIC (acpi_id[0x01] lapic_id[0x00] enabled)

Processor #0 15:5 APIC version 16

ACPI: LAPIC (acpi_id[0x02] lapic_id[0x01] enabled)

Processor #1 15:5 APIC version 16

ACPI: IOAPIC (id[0x02] address[0xfec00000] gsi_base[0])

IOAPIC[0]: Assigned apic_id 2

IOAPIC[0]: apic_id 2, version 17, address 0xfec00000, GSI 0–23

ACPI: IOAPIC (id[0x03] address[0xfebff000] gsi_base[24])

IOAPIC[1]: Assigned apic_id 3

IOAPIC[1]: apic_id 3, version 17, address 0xfebff000, GSI 24–27

ACPI: IOAPIC (id[0x04] address[0xfebfe000] gsi_base[28])

IOAPIC[2]: Assigne