

Panic with amr and 5.4-PRERELEASE

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/stable/2005-03/0413.html>

From: Philippe PEGON (*Philippe.Pegon_at_crc.u-strasbg.fr*)

Date: 03/12/05

Date: Sat, 12 Mar 2005 11:23:43 +0100

To: stable@freebsd.org

Hi,

I have a FreeBSD bi-processor box with amr device in FreeBSD 5.4-prerelease of this week.

```
# uname -a
```

```
FreeBSD sokaris2.u-strasbg.fr 5.4-PRERELEASE FreeBSD 5.4-PRERELEASE #3:
```

```
Thu Mar 10 15:33:01 CET 2005
```

```
root@crc.u-strasbg.fr:/usr/obj/usr/src/sys/SOKARIS2 i386
```

Starting a program which continuously polls the state of the raid array (amrstat, see source attached), and making a buildworld at the same time triggers a kernel panic. The problem is fairly easy to reproduce.

Features added in the SMP kernel : altq, KDB, DDB, GDB (see config file and dmesg output attached). The kernel is launched with ACPI disabled.

A stack trace of the kernel panic and the result of a remote gdb follow.

Thank you by advance for your help,

Philippe PEGON

PANIC

lock order reversal

1st 0xc239994c AMR IO Lock (AMR IO Lock) @ /usr/src/sys/dev/amr/amr.c:487

2nd 0xc29fdd28 user map (user map) @ /usr/src/sys/vm/vm_map.c:2998

KDB: stack backtrace:

kdb_backtrace(ffffffff,c08d3f20,c08d4970,c086802c,c08f7f58) at

kdb_backtrace+0x29

witness_checkorder(c29fdd28,9,c0821569,bb6,c08ccb60,0,c080cb81,9d) at

witness_checkorder+0x49d

_sx_xlock(c29fdd28,c0821569,bb6) at _sx_xlock+0x2c

_vm_map_lock_read(c29fdce4,c0821569,bb6,28cc360,c2a74b04) at

freebsd-stable: Panic with amr and 5.4-PRERELEASE

```
_vm_map_lock_read+0x37
vm_map_lookup(f157aa6c,0,2,f157aa70,f157aa60) at vm_map_lookup+0x28
vm_fault(c29fdce4,0,2,8,c2a75c80) at vm_fault+0x66
trap_pfault(f157ab34,0,0) at trap_pfault+0xd2
trap(c0600018,c0860010,10,0,c2dbd200) at trap+0x2f1
calltrap() at calltrap+0x5
---- trap 0xc, eip = 0xc04b3696, esp = 0xf157ab74, ebp = 0xf157ab74 ----
amr_releasecmd(0,c2dbd1c0,c0865180,c2ce0800,c0865180) at amr_releasecmd+0x6
amr_ioctl(c08ca0d8,c0304301,c2dbd200,1,c2a75c80) at amr_ioctl+0x2cc
spec_ioctl(f157ac08,f157acb4,c0669396,f157ac08,c08ade40) at spec_ioctl+0x11d
spec_vnoperate(f157ac08) at spec_vnoperate+0x13
vn_ioctl(c26a0dd0,c0304301,c2dbd200,c29cd280,c2a75c80) at vn_ioctl+0x1ee
ioctl(c2a75c80,f157ad14,3,1,293) at ioctl+0x344
syscall(2f,2f,2f,bfbfed00,bfbfecf8) at syscall+0x213
Xint0x80_syscall() at Xint0x80_syscall+0x1f
---- syscall (54, FreeBSD ELF32, ioctl), eip = 0x280aeea4, esp =
0xbfbfe2e4, ebp = 0xbfbfe340 ----
```

```
Fatal trap 12: page fault while in kernel mode
cpuid = 0; apic id = 01
fault virtual address = 0x0
fault code = supervisor write, page not present
instruction pointer = 0x8:0x
```