

# Frequent VFS crashes with RELENG\_6

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/stable/2006-09/msg01019.html>

---

- *From:* "Vlad GALU" <dudu@xxxxxxx>
  - *Date:* Sat, 30 Sep 2006 10:30:12 +0300
- 

I've been getting random crashes like the one below, once or twice a week, always in the same code path. The system is a RELENG\_6 as of Wed Sep 27 11:42:57 EEST 2006, running on amd64.

-- cut here --

#0 doadump () at pcpu.h:172

No locals.

#1 0xffffffff8022d033 in boot (howto=260) at ../../kern/kern\_shutdown.c:409  
first\_buf\_printf = 1

#2 0xffffffff8022d687 in panic (fmt=0xffffffff002bb6e260 "°ö¼") at  
../../kern/kern\_shutdown.c:565

bootopt = 260

newpanic = 0

ap = { {gp\_offset = 16, fp\_offset = 48, overflow\_arg\_area =  
0xfffffffffa7995790, reg\_save\_area = 0xfffffffffa79956b0} }

buf = "vm\_page\_unwire: invalid wire count: 0", '\0' <repeats 218 times>

#3 0xffffffff8036980b in vm\_page\_unwire (m=0xffffffff003e5c79e8,  
activate=0) at ../../vm/vm\_page.c:1265

No locals.

#4 0xffffffff80282c15 in vfs\_vmio\_release (bp=0xffffffff9a6c2430) at  
../../kern/vfs\_bio.c:1470

i = 1

m = 0xffffffff003e5c79e8

#5 0xffffffff80285f78 in getnewbuf (slpflag=0, slptimeo=0, size=0,  
maxsize=16384) at ../../kern/vfs\_bio.c:1779

addr = 18446744072226429136

bp = (struct buf \*) 0xffffffff9a6c2430

nbp = (struct buf \*) 0xffffffff9a69ac48

defrag = 0

nqindex = 1

flushingbufs = 0

#6 0xffffffff802863c0 in getblk (vp=0xffffffff001015c5d0, blkno=0,  
size=2048, slpflag=0, slptimeo=0, flags=0) at  
../../kern/vfs\_bio.c:2486

bsize = 0

maxsize = 0

vmio = 1

offset = 0

bp = (struct buf \*) 0x0

## Frequent VFS crashes with RELENG\_6

```
bo = (struct bufobj *) 0xffffffff001015c720
#7 0xffffffff802880ec in breadn (vp=0xffffffff001015c5d0, blkno=0,
size=0, rablkn=0x0, rabsz=0x0, cnt=0, cred=0x0, bpp=0x0) at
../../../../kern/vfs_bio.c:738
bp = (struct buf *) 0xfffffffffa79958f0
rabp = (struct buf *) 0x344
i = -1
rv = 0
readwait = 0
#8 0xffffffff8028850e in bread (vp=0x0, blkno=0, size=0, cred=0x0,
bpp=0x0) at ../../../../kern/vfs_bio.c:719
No locals.
#9 0xffffffff803427a5 in ffs_read (ap=0x0) at ../../../../ufs/ffs/ffs_vnops.c:523
vp = (struct vnode *) 0xffffffff001015c5d0
ip = (struct inode *) 0xffffffff0017978780
uio = (struct uio *) 0xfffffffffa7995b50
fs = (struct fs *) 0xffffffff0012347000
bp = (struct buf *) 0x0
lbn = 0
nextlbn = 1
bytesinfile = 0
size = 2048
xfersize = 836
blkoffset = 0
error = 0
orig_resid = 4096
seqcount = 2
ioflag = 131072
#10 0xffffffff803b374a in VOP_READ_APV (vop=0x0, a=0x0) at vnode_if.c:643
rc = 0
#11 0xffffffff802a74e0 in vn_read (fp=0xffffffff001e5f8078,
uio=0xfffffffffa7995b50, active_cred=0x0, flags=0,
td=0xffffffff002bb6e260) at vnode_if.h:343
vp = (struct vnode *) 0xffffffff001015c5d0
error = 0
ioflag = 131072
#12 0xffffffff80257b64 in dofileread (td=0xffffffff002bb6e260, fd=5,
fp=0xffffffff001e5f8078, auio=0xfffffffffa7995b50, offset=0, flags=0) at
file.h:240
cnt = 4096
error = 509575288
ktruiio = (struct uio *) 0x0
#13 0xffffffff80257de0 in kern_readv (td=0xffffffff002bb6e260, fd=5,
auio=0xfffffffffa7995b50) at ../../../../kern/sys_generic.c:192
fp = (struct file *) 0xffffffff001e5f8078
error = 0
#14 0xffffffff80257eda in read (td=0x0, uap=0x0) at
../../../../kern/sys_generic.c:116
auio = {uio_iov = 0xfffffffffa7995b40, uio_iovcnt = 1,
uio_offset = 0, uio_resid = 4096, uio_segflg = UIO_USERSPACE, uio_rw =
UIO_READ, uio_td = 0xffffffff002bb6e260}
```

## Frequent VFS crashes with RELENG\_6

```
aiov = {iov_base = 0x666000, iov_len = 4096}
#15 0xffffffff8038b2d8 in syscall (frame=
{tf_rdi = 5, tf_rsi = 6709248, tf_rdx = 4096, tf_rcx =
542953472, tf_r8 = 1, tf_r9 = 0, tf_rax = 3, tf_rbx = 6151168, tf_rbp
= 4294967295, tf_r10 = 3260, tf_r11 = 518, tf_r12 = 0, tf_r13 =
140737488327200, tf_r14 = 140737488327328, tf_r15 = 5, tf_trapno = 12,
tf_addr = 9093168, tf_flags = 0, tf_err = 2, tf_rip = 550694412, tf_cs
= 43, tf_rflags = 518, tf_rsp = 140737488327160, tf_ss = 35}) at
../././amd64/amd64/trap.c:792
params = 0x7fffffff9200 <Address 0x7fffffff9200 out of bounds>
callp = (struct sysent *) 0xffffffff80502ae8
p = (struct proc *) 0xffffffff0022bef6b0
orig_tf_rflags = 518
sticks = 116
error = 0
narg = 3
args = {5, 6709248, 4096, 542953472, 1, 0, 140737488327328, 5}
argp = (register_t *) 0x0
code = 3
reg = 48
regcnt = 6
#16 0xffffffff80377bc8 in Xfast_syscall () at
../././amd64/amd64/exception.S:270
-- and here --
```

--

If it's there, and you can see it, it's real.  
If it's not there, and you can see it, it's virtual.  
If it's there, and you can't see it, it's transparent.  
If it's not there, and you can't see it, you erased it.

---

freebsd-stable@xxxxxxxxxxxxx mailing list

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

To unsubscribe, send any mail to "freebsd-stable-unsubscribe@xxxxxxxxxxxxx"