Hello,

I tried loading the efirt module then running efivar but got a panic.

Got the following backtrace when using the dump I got (kgdb then bt):

```
(kgdb) bt
#0  _get_mycpu () at ./machine/thread.h:69
#1  panic (fmt=fmt@entry=0xffffffff805dce3e "%s") at /usr/src/sys/kern/kern_shutdown.c:868
#2  0xffffffff8058333e in trap_fatal (frame=frame@entry=0xffffffff800bc3195e8, eva=2129260136) at /usr/src/sys/platform/pc64/x66_64/trap.c:1116
#3  0xffffffff8058374c in trap_pfault (frame=0xffffffff800bc3195e8, usermode=0) at /usr/src/sys/platform/pc64/x66_64/trap.c:943
#4  0xffffffff805f9ea in calltrap () at /usr/src/sys/platform/pc64/x66_64/exception.S:321
#5  0xffffffff802000d53 in efi_var_nextname (namesize=namesize@entry=0xffffffff800bc319870, name=name@entry=0xffffffff800bc8f2c00, vendor=vendor@entry=0xffffffff800bc319878) at /usr/src/sys/dev/misc/efirt/../platform/pc64/x66_64/efirt.c:562
#6  0xffffffff8002001f3 in efidev_ioctl (ap=<optimized out>) at /usr/src/sys/dev/misc/efirt/efidev.c:146
#7  0xffffffff8002063d5 in dev_ioctl (dev=dev@entry=0xffffffff80066c86700, cmd=cmd@entry=3224913157, data=data@entry=0xffffffff800bc319868 "", fflag=<optimized out>, cred=cred@entry=0xffffffff8004676db0, msg=msg@entry=0xffffffff800bc319960, fp=0xffffffff80770f1d00) at /usr/src/sys/kern/kern_device.c:251
#8  0xffffffff80402e555 in devfs_fo_ioctl (fp=0xffffffff80077f1d00, com=3224913157, data=0xffffffff800bc319868 ",", ucred=0xffffffff8004676db0, msg=0xffffffff800bc319960) at /usr/src/sys/vfs/devfs/devfs_vnop.c:1548
#9  0xffffffff80321d1b in fo_ioctl (msg=0xffffffff800bc319960, cred=<optimized out>, data=<optimized out>, com=<optimized out>, fp=0xffffffff80770f1d00) at /usr/src/sys/sys/file2.h:84
#10 mapped_ioctl (fd=<optimized out>, com=<optimized out>, uspc_data=<optimized out>, map=0x0, msg=<optimized out>) at /usr/src/sys/kern/sys_genetic.c:717
#11 0xffffffff805848566 in syscall2 (frame=0xffffffff800bc3199f8) at /usr/src/sys/platform/pc64/x66_64/trap.c:1317
#12 0xffffffff805610fd in Xfast_syscall () at /usr/src/sys/platform/pc64/x66_64/exception.S:450
#13 0x000000000000000b in ?? ()

```

Backtrace stopped: previous frame inner to this frame (corrupt stack?)

Is that enough info?

History

#1 - 05/28/2020 03:30 PM - swildner
FWIW, I have bisected it and the first bad commit is this one:

https://gitweb.dragonflybsd.org/dragonfly.git/commitdiff/921ef7b6495969fa8fb02d6b7ec9b34d60c01c6c

#2 - 05/28/2020 10:11 PM - dillon

Looks like it may be trying to access a userspace address without using copyout(). SMAP caught it. I'm looking at it now.

-Matt

#3 - 05/28/2020 11:57 PM - dillon
- Status changed from New to Closed

Fix pushed to master and cherry-picked over to release. The SMAP/SMEP protections were interfering with the EFI code, both have to be disabled.
along with additional failsafe checks done in trap() to allow the page fault to proceed. This is because the direct mapping for the EFI address space uses user-space addresses.

-Matt