DragonFlyBSD - Bug #3052

panic DragonFly v4.8.1-RELEASE by mounting a malformed NTFS image [64.000]

08/14/2017 03:22 AM - open.source@ribose.com

Status:	New	**Start date:**	08/14/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Kernel	**Estimated time:**	0.00 hour
Target version:	Latest stable		

Description

It is possible to panic DragonFly v4.8.1-RELEASE by mounting a malformed NTFS image.

kgdb kern.1 vmcore.1
GNU gdb (GDB) 7.6.1
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-dragonfly".
For bug reporting instructions, please see:
<http://bugs.dragonflybsd.org/>...
Reading symbols from /var/crash/kern.1...done.

Unread portion of the kernel message buffer:
Copyright (c) 2003-2017 The DragonFly Project.
Copyright (c) 1992-2003 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
DragonFly v4.8.1-RELEASE #5: Tue Aug 1 23:19:38 EDT 2017
root@www.shiningsilence.com:/usr/obj/home/justin/release/4_8/sys/X86_64_GENERIC
i8254 clock: 1193169 Hz
TSC invariant clock: 2294698033 Hz
CPU: Intel(R) Core(TM) i7-4850HQ CPU @ 2.30GHz (2294.70-MHz K8-class CPU)
Origin = "GenuineIntel" Id = 0x40661 Stepping = 1
Features=0x783fbff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CMOV,PAT,PSE36,MMX,FXSR,SSE,SSE2>
Features2=0x56d8220b<SSE3,PCLMULQDQ,MON,SSSE3,CX16,SSE4.1,SSE4.2,MOVBE,POPCNT,AESNI,XSAVE,AVX,RDRND>
AMD Features=0x28100800<SYSCALL,NX,RDTSCP,LM>
AMD Features2=0x21<LAHF,ABM>
Structured Extended Features=0x2000
real memory = 132709376 (126 MB)
avail memory = 81620992 (77 MB)
lapic: divisor index 0, frequency 500004126 Hz
srat_probe: can't locate SRAT
SMI Frequency (worst case): 10309 Hz (97 us)
Initialize MI interrupts
TSC: cputimer freq 71709313, shift 5
VMM: VMX is not supported by this Intel CPU
wdog: In-kernel automatic watchdog reset enabled
kbd1 at kbdmux0
md0: Malloc disk
interrupt uses mplock: swi_taskq
ACPI: RSDP 0x00000000000E0000 000024 (v02 VBOX)
ACPI: XSDT 0x0000000007FF0030 00003C (v01 VBOX   VBOXXSDT 00000001 ASL 00000061)
ACPI: FACP 0x0000000007FF00F0 0000F4 (v04 VBOX   VBOXFACP 00000001 ASL 00000061)
ACPI: DSDT 0x0000000007FF0470 0021C8 (v02 VBOX   VBOXBIOS 00000002 INTL 20100528)
ACPI: FACS 0x0000000007FF0200 000040
ACPI: FACS 0x0000000007FF0200 000040
ACPI: APIC 0x0000000007FF0240 000054 (v02 VBOX   VBOXAPIC 00000001 ASL 00000061)
ACPI: SSDT 0x0000000007FF02A0 0001CC (v01 VBOX   VBOXCPUT 00000002 INTL 20100528)
cryptosoft0: <software crypto> on motherboard

```
aesni0: <AES-CBC,AES-XTS> on motherboard
padlock0: No ACE support.
rdrand0: <RdRand RNG> on motherboard
acpi0: <VBOX VBOXXSDT> on motherboard
ACPI: Executed 1 blocks of module-level executable AML code
ACPI: 2 ACPI AML tables successfully acquired and loaded
ACPI FADT: SCI testing interrupt mode ...
ACPI FADT: SCI select level/high
acpi0: Power Button (fixed)
acpi0: Sleep Button (fixed)
acpi_timer0 on acpi0
pcib0: <ACPI Host-PCI bridge> port 0xcf8-0xcff on acpi0
pci0: <ACPI PCI bus> on pcib0
isab0: <PCI-ISA bridge> at device 1.0 on pci0
isa0: <ISA bus> on isab0
atapci0: <Intel PIIX4 UDMA33 controller> port 0xd000-0xd00f,0x376,0x170-0x177,0x3f6,0x1f0-0x1f7 at device 1.1 on pci0
ata0: <ATA channel 0> on atapci0
interrupt uses mplock: ata0
ad0: 16384MB <VBOX HARDDISK 1.0> at ata0-master UDMA33
ata1: <ATA channel 1> on atapci0
interrupt uses mplock: ata1
acd0: DVDROM <VBOX CD-ROM/1.0> at ata1-master UDMA33
vgapci0: <VGA-compatible display> mem 0xe0000000-0xe0ffffff irq 18 at device 2.0 on pci0
vgapci0: Boot video device
em0: <Intel(R) PRO/1000 Network Connection 82540EM 7.4.2> port 0xd010-0xd017 mem 0xf0000000-0xf001ffff irq 19 at device 3.0
on pci0
em0: MAC address: 08:00:27:b2:31:f4
pci0: <base peripheral> (vendor 0x80ee, dev 0xcafe) at device 4.0 irq 20
ohci0: <Apple KeyLargo/Intrepid USB controller> mem 0xf0804000-0xf0804fff irq 22 at device 6.0 on pci0
usbus0 on ohci0
pci0: <bridge> (vendor 0x8086, dev 0x7113) at device 7.0 irq 23
usbus0: 12Mbps Full Speed USB v1.0
ehci0: <Intel 82801FB (ICH6) USB 2.0 controller> mem 0xf0805000-0xf0805fff irq 19 at device 11.0 on pci0
usbus1: EHCI version 1.0
ugen0.1: <Apple> at usbus0
uhub0: <Apple OHCI root HUB, class 9/0, rev 1.00/1.00, addr 1> on usbus0
usbus1 on ehci0
battery0: <ACPI Control Method Battery> on acpi0
acpi_acad0: <AC Adapter> on acpi0
atkbdc0: <Keyboard controller (i8042)> port 0x64,0x60 irq 1 on acpi0
atkbd0: <AT Keyboard> irq 1 on atkbdc0
kbd0 at atkbd0
usbus1: 480Mbps High Speed USB v2.0
ugen1.1: <Intel> at usbus1
uhub1: <Intel EHCI root HUB, class 9/0, rev 2.00/1.00, addr 1> on usbus1
psm0: <PS/2 Mouse> irq 12 on atkbdc0
interrupt uses mplock: psm0
psm0: model IntelliMouse Explorer, device ID 4
cpu0: <ACPI CPU> on acpi0
cpu_cst0: <ACPI CPU C-State> on cpu0
ACPI: Enabled 2 GPEs in block 00 to 07
orm0: <ISA Option ROMs> at iomem 0xc0000-0xc7fff,0xe2000-0xe2fff on isa0
pmtimer0 on isa0
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff on isa0
sc0: <System console> at flags 0x500 on isa0
sc0: VGA <16 virtual consoles, flags=0x300>
sio0: can't drain, serial port might not exist, disabling
sio1: can't drain, serial port might not exist, disabling
hpt27xx: no controller detected.
CAM: Configuring 2 busses
uhub0: 12 ports with 12 removable, self powered
CAM: finished configuring all busses
cd0 at ata1 bus 0 target 0 lun 0
cd0: <VBOX CD-ROM 1.0> Removable CD-ROM SCSI-0 device
cd0: 33.000MB/s transfers
cd0: Attempt to query device size failed: NOT READY, Medium not present
uhub1: 12 ports with 12 removable, self powered
```

```
no B_DEVMAGIC (bootdev=0)
Mounting root from ufs:serno/VB72453a18-bfd99f8c.s1d
DMA space used: 160k, remaining available: 1248k
Mounting devfs
<118>Loading configuration files.
<118>Loading devfs rules:
<118> /etc/defaults/devfs.conf
<118>.
<118>Initializing random seed:
<118>done.
<118>dumpon: crash dumps to /dev/ad0s1b (21, 0x20001)
<118>Starting file system checks:
<118>/dev/serno/VB72453a18-bfd99f8c.s1d:
<118>FILESYSTEM CLEAN; SKIPPING CHECKS
<118>/dev/serno/VB72453a18-bfd99f8c.s1d:
<118>clean, 11841703 free
<118>(2783 frags, 1479865 blocks, 0.0% fragmentation)
<118>/dev/serno/VB72453a18-bfd99f8c.s1a:
<118>FILESYSTEM CLEAN; SKIPPING CHECKS
<118>/dev/serno/VB72453a18-bfd99f8c.s1a:
<118>clean, 438163 free
<118>(155 frags, 54751 blocks, 0.0% fragmentation)
<118>Setting hostname: foobar.localdomain.
<118>starting dhclient on em0
<118>lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
<118>   options=43<RXCSUM,TXCSUM,RSS>
<118>   inet 127.0.0.1 netmask 0xff000000
<118>   inet6 ::1 prefixlen 128
<118>   inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
<118>em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
<118>   options=1b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING>
<118>   inet6 fe80::a00:27ff:feb2:31f4%em0 prefixlen 64 tentative scopeid 0x1
<118>   ether 08:00:27:b2:31:f4
<118>   media: Ethernet autoselect <rxpause> (none)
<118>   status: no carrier
<118>Additional routing options:
<118>.
<118>Starting devd.
<118>Mounting NFS file systems:
<118>.
<118>Building databases...
<118>Starting syslogd.
<118>Aug 15 02:12:57 foobar syslogd: kernel boot file is /boot/kernel/kernel
<118>No core dumps found.
swap low/high-water marks set to 16760/25140
<118>swapon: adding /dev/serno/VB72453a18-bfd99f8c.s1b as swap device
<118>ELF ldconfig path: /lib /usr/lib /usr/local/lib /usr/local/libdata/ldconfig/perl5
<118>Id  Refs Name
<118>208    1 nfs
<118>NFS CLIENT:
<118> access_cache_timeout=5
<118> neg_cache_timeout=3
<118>.
<118>Starting local daemons:
<118>.
<118>Updating motd.
<118>Configuring syscons:
<118> blanktime
<118>.
<118>Starting sshd.
<118>sendmail_submit: /etc/mail/aliases.db not present, generating
<118>newaliases: no recipients
<118>sendmail_clientmqueue: /etc/mail/aliases.db not present, generating
<118>newaliases: no recipients
<118>Starting cron.
<118>Local package initialization:
<118>.
```

<118>Additional TCP options:
<118>.
<118>
<118>Tue Aug 15 02:12:58 HKT 2017
<118>Aug 15 02:13:23 foobar login: ROOT LOGIN (root) ON ttyv0

Fatal trap 12: page fault while in kernel mode
cpuid = 0; lapic->id = 00000000
fault virtual address = 0xfffffffffffffff8
fault code = supervisor read data, page not present
instruction pointer = 0x8:0xffffffff82c02f21
stack pointer = 0x10:0xffffff8051df4078
frame pointer = 0x10:0xffffff8051df40d8
code segment = base 0x0, limit 0xfffff, type 0x1b
= DPL 0, pres 1, long 0, def32 0, gran 1
processor eflags = interrupt enabled, resume, IOPL = 0
current process = 959
current thread = pri 6
kernel: type 12 trap, code=0

CPU0 stopping CPUs: 0x00000000
stopped
Physical memory: 87 MB
Dumping 1106 MB: 1091 1075 1059 1043 1027 1011 995 979 963 947 931 915 899 883 867 851 835 819 803 787 771 755 739 723 707 691 675 659 643 627 611 595 579 563 547 531 515 499 483 467 451 435 419 403 387 371 355 339 323 307 291 275 259 243 227 211 195 179 163 147 131 115 99 83 67 51 35 19 3

[New kernel syncer14]
[New pid 959/0, mount_ntfs]
[New pid 958/0, mount]
[New pid 956/0, sh]
[New pid 952/0, csh]
[New pid 500/0, syslogd]
[New pid 410/0, dhclient]
[New pid 941/0, getty]
[New pid 940/0, getty]
[New pid 939/0, getty]
[New pid 938/0, getty]
[New pid 937/0, getty]
[New pid 936/0, getty]
[New pid 935/0, getty]
[New pid 934/0, login]
[New kernel syscons7]
[New kernel syscons6]
[New kernel syscons5]
[New kernel syscons4]
[New kernel syscons3]
[New kernel syscons2]
[New kernel syscons1]
[New pid 840/0, cron]
[New pid 806/0, sshd]
[New pid 435/0, devd]
[New pid 277/0, dhclient]
[New pid 276/0, dhclient]
[New kernel syncer13]
[New kernel syncer12]
[New kernel syncer5]
[New kernel syscons255]
[New kernel syncer4]
[New pid 1/0, init]
[New kernel consttyd]
[New kernel vnlru]
[New kernel bufdaemon_hw]
[New kernel bufdaemon]
[New kernel vmdaemon]
[New kernel swapcached]
[New kernel pagedaemon]

[New kernel syncer3]
[New kernel unp taskq]
[New kernel random]
[New kernel syncer2]
[New kernel syncer1]
[New kernel ithread12 0]
[New kernel ithread1 0]
[New kernel usbus1]
[New kernel usbus1]
[New kernel usbus1]
[New kernel usbus1]
[New kernel usbus0]
[New kernel usbus0]
[New kernel usbus0]
[New kernel usbus0]
[New kernel ithread22 0]
[New kernel ithread19 0]
[New kernel ithread15 0]
[New kernel ithread14 0]
[New kernel ithread9 0]
[New kernel acpi_task]
[New kernel ithread197 0]
[New kernel ithread195 0]
[New kernel xpt_thrd]
[New kernel crypto returns]
[New kernel crypto 0]
[New kernel firmware taskq]
[New kernel sensors 0]
[New kernel taskq_cpu 0]
[New kernel ifnet 0]
[New kernel disk_msg_core]
[New kernel netisr_cpu 0]
[New kernel devfs_msg_core]
[New kernel dsched 0]
[New kernel usched 0]
[New kernel usched 0]
[New kernel ithread196 0]
[New kernel ithreadE 0]
[New kernel softclock 0]
[New pid 0/0, swapper]
[New kernel idle_0]
Reading symbols from /boot/kernel/acpi.ko...(no debugging symbols found)...done.
Loaded symbols for /boot/kernel/acpi.ko
Reading symbols from /boot/kernel/ehci.ko...(no debugging symbols found)...done.
Loaded symbols for /boot/kernel/ehci.ko
Reading symbols from /boot/kernel/xhci.ko...(no debugging symbols found)...done.
Loaded symbols for /boot/kernel/xhci.ko
Reading symbols from /boot/kernel/ntfs.ko...(no debugging symbols found)...done.
Loaded symbols for /boot/kernel/ntfs.ko
_get_mycpu () at ./machine/thread.h:69
69   ./machine/thread.h: No such file or directory.
(kgdb) bt
#0 _get_mycpu () at ./machine/thread.h:69
#1 md_dumpsys (di=0xffffffff81312f20 <dumper>) at /home/justin/release/4_8/sys/platform/pc64/x86_64/dump_machdep.c:275
#2 0xffffffff802b5ee8 in db_fncall (dummy1=<optimized out>, dummy2=<optimized out>, dummy3=<optimized out>,
dummy4=<optimized out>)
at /home/justin/release/4_8/sys/ddb/db_command.c:558
#3 0xffffffff802b63a4 in db_command (last_cmdp=0xffffffff812c7370 <db_last_command>, cmd_table=<optimized out>,
aux_cmd_tablep=<optimized out>,
aux_cmd_tablep_end=<optimized out>) at /home/justin/release/4_8/sys/ddb/db_command.c:400
#4 db_command_loop () at /home/justin/release/4_8/sys/ddb/db_command.c:467
#5 0xffffffff802b9742 in db_trap (type=type@entry=12, code=code@entry=0) at /home/justin/release/4_8/sys/ddb/db_trap.c:71
#6 0xffffffff80a54576 in kdb_trap (type=type@entry=12, code=code@entry=0, regs=regs@entry=0xffffff8051df3fa8)
at /home/justin/release/4_8/sys/platform/pc64/x86_64/db_interface.c:176
#7 0xffffffff80a5afaf in trap_fatal (frame=frame@entry=0xffffff8051df3fa8, eva=<optimized out>)
at /home/justin/release/4_8/sys/platform/pc64/x86_64/trap.c:1018
#8 0xffffffff80a5b3ff in trap_pfault (frame=0xffffff8051df3fa8, usermode=0) at

```
/home/justin/release/4_8/sys/platform/pc64/x86_64/trap.c:923
#9  0xffffffff80a5b8da in trap (frame=0xffffff8051df3fa8) at /home/justin/release/4_8/sys/platform/pc64/x86_64/trap.c:603
#10 0xffffffff80a4403f in calltrap () at /home/justin/release/4_8/sys/platform/pc64/x86_64/exception.S:188
#11 0xffffffff82c02f21 in ntfs_procfixups () from /boot/kernel/ntfs.ko
#12 0xffffffff82c03f64 in ntfs_loadntnode () from /boot/kernel/ntfs.ko
#13 0x0000000000000000 in ?? ()
(kgdb) info reg
rax            *value not available*
rbx            0x0      0
rcx            *value not available*
rdx            *value not available*
rsi            *value not available*
rdi            *value not available*
rbp            0xffffff8051df3ca8       0xffffff8051df3ca8
rsp            0xffffff8051df3ba0       0xffffff8051df3ba0
r8             *value not available*
r9             *value not available*
r10            *value not available*
r11            *value not available*
r12            0x0      0
r13            0xffffffff805e5610       -2141301232
r14            0xffffffff80c035f8       -2134886920
r15            0xffffffff80c036b0       -2134886736
rip            0xffffffff80a555a6       0xffffffff80a555a6 <md_dumpsys+630>
eflags          *value not available*
cs             *value not available*
ss             *value not available*
ds             *value not available*
es             *value not available*
fs             *value not available*
gs             *value not available*
(kgdb)
```

A copy of the malformed msdosfs image + the above kgdb output can be found here:
https://github.com/riboseinc/fuzzbsd/tree/master/results/dragonflybsd_4.8.1/ntfs/64

This submission is in response to the Ribose Retrace Challenge. The Bug Challenge encourages finding bugs (any bug AND security vulnerabilities) in well-known software (OSS / proprietary) using retrace (https://github.com/riboseinc/retrace).

Files

kgdb.txt	13.6 KB	08/14/2017	open.source@ribose.com
image-fuzzbsd-ntfs-64.000	1 MB	08/14/2017	open.source@ribose.com