DragonFlyBSD - Bug #1873

Panic upon usb mouse detach and reattaching

10/16/2010 06:16 PM - rumcic

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

After several detaches and reattaches, the machine paniced with "Fatal trap 12:
page fault while in kernel mode"

The core dump is available at leaf:~rumko/crash/ums/*.0

#0 _get_mycpu (di=0xc04ff620) at ./machine/thread.h:83
#1 md_dumpsys (di=0xc04ff620)
at /usr/src/sys/platform/pc32/i386/dump_machdep.c:263
#2 0xc01e46cd in dumpsys () at /usr/src/sys/kern/kern_shutdown.c:880
#3 0xc01e4c8d in boot (howto=260) at /usr/src/sys/kern/kern_shutdown.c:387
#4 0xc01e4f56 in panic (fmt=0xc0443534 "%s")
at /usr/src/sys/kern/kern_shutdown.c:786
#5 0xc040ffcb in trap_fatal (frame=0xea434808, eva=<value optimized out>)
at /usr/src/sys/platform/pc32/i386/trap.c:1117
#6 0xc04100d9 in trap_pfault (frame=0xea434808, usermode=0, eva=12)
at /usr/src/sys/platform/pc32/i386/trap.c:1018
#7 0xc0410b44 in trap (frame=0xea434808)
at /usr/src/sys/platform/pc32/i386/trap.c:699
#8 0xc03fcf17 in calltrap ()
at /usr/src/sys/platform/pc32/i386/exception.s:785
#9 0xc01d0854 in knote_remove (klist=0xd4292224, kn=0xea366ea0)
at /usr/src/sys/kern/kern_event.c:1370
#10 0xc0312c44 in devfs_detached_filter_detach (kn=0xea366ea0)
at /usr/src/sys/vfs/devfs/devfs_core.c:2234
#11 0xc01d0de7 in knote_detach_and_drop (kn=0xea366ea0)
at /usr/src/sys/kern/kern_event.c:1258
#12 0xc01d157b in kqueue_register (kq=0xea3965b4, kev=0xea4348b8)
at /usr/src/sys/kern/kern_event.c:933
#13 0xc020b2f3 in poll_copyout (arg=0xea434c9c, kevp=0xea4349b4, count=2,
res=0xea434cf0) at /usr/src/sys/kern/sys_generic.c:1325
#14 0xc01d20c5 in kern_kevent (kq=0xea3965b4, nevents=2147483647,
res=0xea434cf0, uap=0xea434c9c, kevent_copyinfn=0xc020b4a5 <poll_copyin>,
kevent_copyoutfn=0xc020b290 <poll_copyout>, tsp_in=0xea434cb0)
at /usr/src/sys/kern/kern_event.c:697
#15 0xc020b031 in dopoll (uap=0xea434cf0)
at /usr/src/sys/kern/sys_generic.c:1474
#16 sys_poll (uap=0xea434cf0) at /usr/src/sys/kern/sys_generic.c:1228
#17 0xc04113d2 in syscall2 (frame=0xea434d40)
at /usr/src/sys/platform/pc32/i386/trap.c:1310
#18 0xc03fcfc6 in Xint0x80_syscall ()
at /usr/src/sys/platform/pc32/i386/exception.s:876
#19 0x0000001f in ?? ()
--
Please do not CC me, since I already receive everything from these MLs.

Regards,
Rumko

History

#1 - 01/29/2011 04:22 PM - rumcic

A workaround has been provided by sjg ... by commenting out knote_remove, the

panic will not occur but small amounts of memory will be leaked.

#2 - 01/29/2011 09:57 PM - nthery

Could you make vmcore.0 and info.0 readable please?

On 16 October 2010 20:13, Rumko <rumcic@gmail.com> wrote:
> After several detaches and reattaches, the machine paniced with "Fatal trap 12:
> page fault while in kernel mode"
>
> The core dump is available at leaf:~rumko/crash/ums/*.0
>
> #0 _get_mycpu (di=0xc04ff620) at ./machine/thread.h:83
> #1 md_dumpsys (di=0xc04ff620)
> at /usr/src/sys/platform/pc32/i386/dump_machdep.c:263
> #2 0xc01e46cd in dumpsys () at /usr/src/sys/kern/kern_shutdown.c:880
> #3 0xc01e4c8d in boot (howto=260) at /usr/src/sys/kern/kern_shutdown.c:387
> #4 0xc01e4f56 in panic (fmt=0xc0443534 "%s")
> at /usr/src/sys/kern/kern_shutdown.c:786
> #5 0xc040ffcb in trap_fatal (frame=0xea434808, eva=<value optimized out>)
> at /usr/src/sys/platform/pc32/i386/trap.c:1117
> #6 0xc04100d9 in trap_pfault (frame=0xea434808, usermode=0, eva=12)
> at /usr/src/sys/platform/pc32/i386/trap.c:1018
> #7 0xc0410b44 in trap (frame=0xea434808)
> at /usr/src/sys/platform/pc32/i386/trap.c:699
> #8 0xc03fcf17 in calltrap ()
> at /usr/src/sys/platform/pc32/i386/exception.s:785
> #9 0xc01d0854 in knote_remove (klist=0xd4292224, kn=0xea366ea0)
> at /usr/src/sys/kern/kern_event.c:1370
> #10 0xc0312c44 in devfs_detached_filter_detach (kn=0xea366ea0)
> at /usr/src/sys/vfs/devfs/devfs_core.c:2234
> #11 0xc01d0de7 in knote_detach_and_drop (kn=0xea366ea0)
> at /usr/src/sys/kern/kern_event.c:1258
> #12 0xc01d157b in kqueue_register (kq=0xea3965b4, kev=0xea4348b8)
> at /usr/src/sys/kern/kern_event.c:933
> #13 0xc020b2f3 in poll_copyout (arg=0xea434c9c, kevp=0xea4349b4, count=2,
> res=0xea434cf0) at /usr/src/sys/kern/sys_generic.c:1325
> #14 0xc01d20c5 in kern_kevent (kq=0xea3965b4, nevents=2147483647,
> res=0xea434cf0, uap=0xea434c9c, kevent_copyinfn=0xc020b4a5 <poll_copyin>,
>   kevent_copyoutfn=0xc020b290 <poll_copyout>, tsp_in=0xea434cb0)
> at /usr/src/sys/kern/kern_event.c:697
> #15 0xc020b031 in dopoll (uap=0xea434cf0)
> at /usr/src/sys/kern/sys_generic.c:1474
> #16 sys_poll (uap=0xea434cf0) at /usr/src/sys/kern/sys_generic.c:1228
> #17 0xc04113d2 in syscall2 (frame=0xea434d40)
> at /usr/src/sys/platform/pc32/i386/trap.c:1310
> #18 0xc03fcfc6 in Xint0x80_syscall ()
> at /usr/src/sys/platform/pc32/i386/exception.s:876
> #19 0x0000001f in ?? ()
> --
> Please do not CC me, since I already receive everything from these MLs.
>
> Regards,
> Rumko
>

#3 - 02/01/2011 09:40 AM - nthery

It tries to read at address 0xC which is the offset of kn_next so
it probably crashes while dereferencing kn_next in SLIST_REMOVE().
This could happen if SLIST_REMOVE() reaches the end of the list
without finding the knode in the klist. I can't figure out how this
could happen though.

Could you chmod vmcore.0 so I can analyse the dump please?

On 16 October 2010 20:13, Rumko <rumcic@gmail.com> wrote:
> After several detaches and reattaches, the machine paniced with "Fatal trap 12:
> page fault while in kernel mode"
>
> The core dump is available at leaf:~rumko/crash/ums/*.0
>
> #0 _get_mycpu (di=0xc04ff620) at ./machine/thread.h:83
> #1 md_dumpsys (di=0xc04ff620)
> at /usr/src/sys/platform/pc32/i386/dump_machdep.c:263

> #2 0xc01e46cd in dumpsys () at /usr/src/sys/kern/kern_shutdown.c:880
> #3 0xc01e4c8d in boot (howto=260) at /usr/src/sys/kern/kern_shutdown.c:387
> #4 0xc01e4f56 in panic (fmt=0xc0443534 "%s")
> at /usr/src/sys/kern/kern_shutdown.c:786
> #5 0xc040ffcb in trap_fatal (frame=0xea434808, eva=<value optimized out>)
> at /usr/src/sys/platform/pc32/i386/trap.c:1117
> #6 0xc04100d9 in trap_pfault (frame=0xea434808, usermode=0, eva=12)
> at /usr/src/sys/platform/pc32/i386/trap.c:1018
> #7 0xc0410b44 in trap (frame=0xea434808)
> at /usr/src/sys/platform/pc32/i386/trap.c:699
> #8 0xc03fcf17 in calltrap ()
> at /usr/src/sys/platform/pc32/i386/exception.s:785
> #9 0xc01d0854 in knote_remove (klist=0xd4292224, kn=0xea366ea0)
> at /usr/src/sys/kern/kern_event.c:1370
> #10 0xc0312c44 in devfs_detached_filter_detach (kn=0xea366ea0)
> at /usr/src/sys/vfs/devfs/devfs_core.c:2234
> #11 0xc01d0de7 in knote_detach_and_drop (kn=0xea366ea0)
> at /usr/src/sys/kern/kern_event.c:1258
> #12 0xc01d157b in kqueue_register (kq=0xea3965b4, kev=0xea4348b8)
> at /usr/src/sys/kern/kern_event.c:933
> #13 0xc020b2f3 in poll_copyout (arg=0xea434c9c, kevp=0xea4349b4, count=2,
> res=0xea434cf0) at /usr/src/sys/kern/sys_generic.c:1325
> #14 0xc01d20c5 in kern_kevent (kq=0xea3965b4, nevents=2147483647,
> res=0xea434cf0, uap=0xea434c9c, kevent_copyinfn=0xc020b4a5 <poll_copyin>,
> kevent_copyoutfn=0xc020b290 <poll_copyout>, tsp_in=0xea434cb0)
> at /usr/src/sys/kern/kern_event.c:697
> #15 0xc020b031 in dopoll (uap=0xea434cf0)
> at /usr/src/sys/kern/sys_generic.c:1474
> #16 sys_poll (uap=0xea434cf0) at /usr/src/sys/kern/sys_generic.c:1228
> #17 0xc04113d2 in syscall2 (frame=0xea434d40)
> at /usr/src/sys/platform/pc32/i386/trap.c:1310
> #18 0xc03fcfc6 in Xint0x80_syscall ()
> at /usr/src/sys/platform/pc32/i386/exception.s:876
> #19 0x0000001f in ?? ()
> --
> Please do not CC me, since I already receive everything from these MLs.
>
> Regards,
> Rumko
>

#4 - 02/01/2011 09:53 AM - rumcic

Done

Files

0001-devfs_core.c-workaround-for-issue1873.patch	931 Bytes	01/30/2011	rumcic