

Re: bpf panic

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2006-02/msg00217.html>

- *From:* Kris Kennaway <kris@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 23 Feb 2006 04:17:58 -0500
-

On Thu, Feb 23, 2006 at 03:19:46AM -0500, Kris Kennaway wrote:

I ran tcpdump and killall tcpdump in a loop on 7.0, and after a few minutes it panicked with:

```
Fatal trap 12: page fault while in kernel mode
cpuid = 0; apic id = 00
fault virtual address = 0x8
fault code = supervisor read, page not present
instruction pointer = 0x20:0xc058d0fb
stack pointer = 0x28:0xe5007c04
frame pointer = 0x28:0xe5007c28
code segment = base 0x0, limit 0xffff, type 0x1b
= DPL 0, pres 1, def32 1, gran 1
processor eflags = interrupt enabled, resume, IOPL = 0
current process = 9 (em0 taskq)
[thread pid 9 tid 100019 ]
Stopped at bpf_mtap+0xf: cmpl $0,0x8(%edi)
db> wh
Tracing pid 9 tid 100019 td 0xc63d6340
bpf_mtap(0,c8f46500,1,2,c63d0001) at bpf_mtap+0xf
ether_input(c6455c00,c8f46500,c8f46500,c6588880,1) at ether_input+0x15f
em_rxeof(c656e800,63,1,c06f7be0,c656e9cc) at em_rxeof+0x423
em_handle_rtx(c656e800,1,c06fbfa7,50,c658889c) at em_handle_rtx+0x5b
taskqueue_run(c6588880,c658889c,c06f0e27,0,1) at taskqueue_run+0x104
taskqueue_thread_loop(c656e9dc,e5007d38,c06f5c42,31a,c656e9dc) at
taskqueue_thread_loop+0x6b
fork_exit(c053b5f8,c656e9dc,e5007d38) at fork_exit+0xc5
fork_trampoline() at fork_trampoline+0x8
--- trap 0x1, eip = 0, esp = 0xe5007d6c, ebp = 0 ---
db>
```

On another machine:

```
Memory modified after free 0xce4cb800(2048) val=a028c0de @ 0xce4cb800
Memory modified after free 0xcc889800(2048) val=a028c0de @ 0xcc889800
Memory modified after free 0xce2b1000(2048) val=a020c0de @ 0xce2b1000
```

Re: bpf panic

Fatal trap 12: page fault while in kernel mode

cpuid = 0; apic id = 00

fault virtual address = 0x8

fault code = supervisor read, page not present

instruction pointer = 0x20:0xc05b033b

stack pointer = 0x28:0xf562f860

frame pointer = 0x28:0xf562f884

code segment = base 0x0, limit 0xffff, type 0x1b

= DPL 0, pres 1, def32 1, gran 1

processor eflags = interrupt enabled, resume, IOPL = 0

current process = 29269 (nfsd)

[thread pid 29269 tid 100044]

Stopped at bpf_mtap+0xf: cmpl \$0,0x8(%edi)

db> wh

Tracing pid 29269 tid 100044 td 0xcc532b60

bpf_mtap(0,ce16ae00,4,f562f8ac,f562f8a8) at bpf_mtap+0xf

fxp_encap(cc546000,ce16ae00,c071eeba,4c2,cc53c0f8) at fxp_encap+0x282

fxp_start_body(cc53c000,0,c071eeba,49a,cc53c000) at fxp_start_body+0x22d

fxp_start(cc53c000,138,0,cc53c000) at fxp_start+0x3c

if_start(cc53c000,0,c0732081,180,2afd2) at if_start+0x88

ether_output_frame(cc53c000,ce16ae00,6,f562fad8,f562fa7c) at ether_output_frame+0x1c1

ether_output(cc53c000,ce16ae00,f562fad8,cc869bb8,cc86b1f8) at ether_output+0x4bb

ip_output(ce16ae00,0,f562fad8,0,0) at ip_output+0x8a9

udp_output(cc86b1f8,ce16ae00,cc765750,0,cc532b60) at udp_output+0x545

udp_send(cc863298,0,ce16ae00,cc765750,0) at udp_send+0x41

sosend(cc863298,cc765750,0,ce16ae00,0) at sosend+0x49e

nfsrv_send(cc863298,cc765750,ce16ae00,1ff,0) at nfsrv_send+0xb9

nfssvc_nfsd(cc532b60,0,c07396f8,9a,f562fc78) at nfssvc_nfsd+0x6a6

nfssvc(cc532b60,f562fd04,8,cc532b60,ccb68420) at nfssvc+0x1f0

syscall(3b,3b,3b,0,0) at syscall+0x304

Xint0x80_syscall() at Xint0x80_syscall+0x1f

--- syscall (155, FreeBSD ELF32, nfssvc), eip = 0x280c2173, esp = 0xbfbfe4dc, ebp = 0xbfbfe4f8 ---

db>

Attachment: [pgp0bYqT00vqg.pgp](#)

Description: PGP signature