Qualcomm Linux Modems by Quectel & Co - Bug #1813

cat /dev/snd/* causes kernel oops

09/30/2016 04:00 PM - zecke

Status:	New	**Start date:**	09/30/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

Nice feature to dump memory around the pointers in the registers. Bad crash. :)

```
/ # cat /dev/snd/pcmC0D*
cat: read error: File descriptor in bad state
cat: read error: Invalid argument
cat: read error: File descriptor in bad state
cat: can't open '/dev/snd/pcmC0D11c': Invalid argument
cat: can't open '/dev/snd/pcmC0D12p': Invalid argument
cat: can't open '/dev/snd/pcmC0D13c': Invalid argument
cat: can't open '/dev/snd/pcmC0D14p': Invalid argument
cat: can't open '/dev/snd/pcmC0D15p': No such device
cat: can't open '/dev/snd/pcmC0D16c': No such device
cat: can't open '/dev/snd/pcmC0D17p': No such device
cat: can't open '/dev/snd/pcmC0D18c': No such device
cat: can't open '/dev/snd/pcmC0D19c': No such device
cat: can't open '/dev/snd/pcmC0D19p': No such device
cat: read error: File descriptor in bad state
cat: read error: Invalid argument
cat: can't open '/dev/snd/pcmC0D20c': No such device
cat: can't open '/dev/snd/pcmC0D20p': No such device
cat: can't open '/dev/snd/pcmC0D21p': No such device
cat: can't open '/dev/snd/pcmC0D22c': No such device
cat: can't open '/dev/snd/pcmC0D23p': No such device
cat: can't open '/dev/snd/pcmC0D24c': No such device
cat: can't open '/dev/snd/pcmC0D25c': No such device
cat: read error: File descriptor in bad state
cat: read error: Invalid argument
cat: read error: File descriptor in bad state
cat: read error: Invalid argument

cat: read error: File descriptor in bad state
cat: read error: Invalid argument
cat: read error: Invalid argument
cat: read error: File descriptor in bad state
cat: read error: File descriptor in bad state
cat: read error: Invalid argument
cat: read error: File descriptor in bad state
cat: read error: Invalid argument
Segmentation fault
/ #
/ #
/ # cat /dev/snd/pcmC0D
pcmC0D0c   pcmC0D14p  pcmC0D19p  pcmC0D22c  pcmC0D3c   pcmC0D7c
pcmC0D0p   pcmC0D15p  pcmC0D1c   pcmC0D23p  pcmC0D3p   pcmC0D7p
pcmC0D10c  pcmC0D16c  pcmC0D1p   pcmC0D24c  pcmC0D4c   pcmC0D8c
pcmC0D11c  pcmC0D17p  pcmC0D20c  pcmC0D25c  pcmC0D4p   pcmC0D8p
pcmC0D12p  pcmC0D18c  pcmC0D20p  pcmC0D2c   pcmC0D5p   pcmC0D9c
pcmC0D13c  pcmC0D19c  pcmC0D21p  pcmC0D2p   pcmC0D6c   pcmC0D9p
/ # cat /dev/snd/pcmC0D
pcmC0D0c   pcmC0D14p  pcmC0D19p  pcmC0D22c  pcmC0D3c   pcmC0D7c
pcmC0D0p   pcmC0D15p  pcmC0D1c   pcmC0D23p  pcmC0D3p   pcmC0D7p
```

```
pcmC0D10c  pcmC0D16c  pcmC0D1p   pcmC0D24c  pcmC0D4c   pcmC0D8c
pcmC0D11c  pcmC0D17p  pcmC0D20c  pcmC0D25c  pcmC0D4p   pcmC0D8p
pcmC0D12p  pcmC0D18c  pcmC0D20p  pcmC0D2c   pcmC0D5p   pcmC0D9c
pcmC0D13c  pcmC0D19c  pcmC0D21p  pcmC0D2p   pcmC0D6c   pcmC0D9p
/ # cat /dev/snd/pcmC0D0c
cat: read error: File descriptor in bad state
/ # dmesg -c
[ 3071.760384] asoc: can't open platform msm-host-pcm-voice
[ 3071.765328] asoc: can't open platform msm-host-pcm-voice
[ 3071.770700] asoc: can't open platform msm-host-pcm-voice
[ 3071.778024] asoc: can't open platform msm-host-pcm-voice
[ 3071.785319]  MDM9615 Media2: asoc: MDM9615 Media2 no valid capture route from source to sink
[ 3071.794811]  MDM9615 Media2: asoc: MDM9615 Media2 no valid playback route from source to sink
[ 3071.840774]  MSM VoIP: asoc: MSM VoIP no valid capture route from source to sink
[ 3071.850114]  MSM VoIP: asoc: MSM VoIP no valid playback route from source to sink
[ 3071.857469]  SLIMBUS_0 Hostless: no BE found for SLIMBUS_0_TX
[ 3071.862627]  SLIMBUS_0 Hostless: asoc: SLIMBUS_0 Hostless no valid capture route from source to
 sink
[ 3071.874286]  SLIMBUS_0 Hostless: asoc: SLIMBUS_0 Hostless no valid playback route from source t
o sink
[ 3071.884144] afe_callback: cmd = 0x100df returned error = 0x2
[ 3071.897268] afe_callback: cmd = 0x100df returned error = 0x2
[ 3071.930046]  VoLTE: asoc: VoLTE no valid capture route from source to sink
[ 3071.938806]  VoLTE: asoc: VoLTE no valid playback route from source to sink
[ 3071.945459] soc-audio soc-audio.0: root widget not found
[ 3071.950495] ------------[ cut here ]------------
[ 3071.954646] kernel BUG at /home/sata2/welford.wei_sam_4222/LTE/Qualcomm/MDM9215/EC20_R02/apss/a
pps_proc/kernel/mm/slub.c:3008!
[ 3071.966030] Internal error: Oops - BUG: 0 [#1] PREEMPT
[ 3071.971127] Modules linked in: snd_soc_alc5616
[ 3071.975583] CPU: 0    Not tainted  (3.0.21+ #1)
[ 3071.980100] PC is at kfree+0x5c/0xec
[ 3071.983640] LR is at dsp_add_new_paths+0x31c/0x35c
[ 3071.988432] pc : [<c00e6988>]    lr : [<c02f3588>]    psr: 40000013
[ 3071.988432] sp : c57f7d34  ip : 000057f7  fp : 00000000
[ 3071.999877] r10: c060245c  r9 : 00000000  r8 : 00000000
[ 3072.005096] r7 : c57f6000  r6 : c5b58ae0  r5 : 00000000  r4 : c5893eb8
[ 3072.011597] r3 : 00000000  r2 : c57f7da8  r1 : c087dee0  r0 : 00000000
[ 3072.018098] Flags: nZcv  IRQs on  FIQs on  Mode SVC_32  ISA ARM  Segment user
[ 3072.025209] Control: 10c5387d  Table: 4582c059  DAC: 00000015
[ 3072.030947]
[ 3072.030947] PC: 0xc00e6908:
[ 3072.035189] 6908  e3510000 0a000002 e59f3010 e5930050 ebffffc9 e3a03000 e584306c e8bd8010
[ 3072.043369] 6928  c06b773c e3500010 e1a0300e e92d40f0 e1a02000 98bd80f0 e280c102 e59f10c8
[ 3072.051518] 6948  e28cc502 e1a0c62c e5910000 e24cc701 e24ccb02 e080128c e790028c e3100902
[ 3072.059666] 6968  1591100c e5910000 e3100080 1591000c 1a000006 e5913000 e3130903 1a000000
[ 3072.067846] 6988  e7f001f2 e1a00001 e8bd40f0 eaff7b59 e590c000 e59c6004 e59c4008 e1510004
[ 3072.075995] 69a8  1a000017 e59c5000 e5904014 e7825004 e10f4000 f10c0080 e5905000 e59cc000
[ 3072.084144] 69c8  e5957000 e157000c 1a000008 e595c004 e15c0006 1a000005 e5852000 e28cc001
[ 3072.092323] 69e8  e5905000 e585c004 e3a0c001 ea000000 e3a0c000 e121f004 e35c0000 18bd80f0
[ 3072.100472]
[ 3072.100472] LR: 0xc02f3508:
[ 3072.104715] 3508  e2888001 e5930000 e2853008 ebf93e84 e59d3024 e5850278 e586340c ea000007
[ 3072.112894] 3528  e59d302c e1a00004 e59f108c e0839109 e5993004 e5932004 ebfb56ea ea00000d
[ 3072.121043] 3548  e2899001 ea000007 e59d1014 e3a07f9f e3a08000 e1a09008 e0070197 e2873f66
[ 3072.129192] 3568  e0843003 e58d3018 e59d302c e5932000 e1590002 baffff69 e59d002c ebf7cce8
[ 3072.137371] 3588  e1a00008 e28dd034 e8bd8ff0 c06133e0 c054919e c05491a6 c04e1b90 c054aa07
[ 3072.145520] 35a8  c04287d8 c054aa20 c054aa4e c06b7754 c054aa04 c054aa01 c054aa62 c054aa88
[ 3072.153669] 35c8  e92d4ff7 e3a07f9f e0070197 e3a0301c e0030193 e1a06000 e0809007 e287bf66
[ 3072.161849] 35e8  e1a05001 e3a08000 e5994198 e080b00b e244400c e58d3004 ea000029 e5943000
[ 3072.169998]
[ 3072.169998] SP: 0xc57f7cb4:
[ 3072.174270] 7cb4  c587de08 c060252c c0602540 00000016 00000001 00000000 c03f4464 c050bf86
[ 3072.182419] 7cd4  ffffffff c57f7d1c c0037d14 00000000 c0037a64 00000000 c087dee0 c57f7da8
[ 3072.190568] 7cf4  00000000 c5893eb8 00000000 c5b58ae0 c57f6000 00000000 00000000 c060245c
[ 3072.198748] 7d14  00000000 000057f7 c57f7d34 c02f3588 c00e6988 40000013 ffffffff c5b58ae0
[ 3072.206897] 7d34  c5893eb8 00000000 c5b58ae0 c57f6000 c02f3588 00000016 c03143d4 c5b58800
```

```
[ 3072.215046] 7d54  00000000 0000000d 00000001 00000000 0000000d 00000015 00000000 c52fb400
[ 3072.223225] 7d74  c57f7da8 c52fb400 c5b58c00 c5893eb8 c5b58ae0 c57f6000 c5b58aec 00000000
[ 3072.231374] 7d94  00000001 00000000 c02f55cc c5b58c00 c57f7da8 c52fb400 c57f7dfc 00000000
[ 3072.239523]
[ 3072.239554] R1: 0xc087de60:
[ 3072.243796] de60  00000080 00000001 000c000c c6004b00 00000000 00000000 00100100 00200200
[ 3072.251945] de80  00000080 00000001 000d000d c6004600 00000000 00000000 00100100 00200200
[ 3072.260094] dea0  00000080 00000001 000d000d c6004600 00000000 00000000 00100100 00200200
[ 3072.268273] dec0  00000000 00000001 ffffffff 00000000 00000000 000000f5 00100100 00200200
[ 3072.276422] dee0  00000000 00000000 ffffffff 00000001 00000000 00000100 00100100 00200200
[ 3072.284571] df00  00000080 00000001 000c000c c6004b00 00000000 00000000 00100100 00200200
[ 3072.292751] df20  00000000 00000000 ffffff80 00000000 00000000 c57f9000 c087d538 c0879438
[ 3072.300899] df40  00000080 00000001 000c000c c6004b00 00000000 00000000 00100100 00200200
[ 3072.309079]
[ 3072.309079] R2: 0xc57f7d28:
[ 3072.313321] 7d28  40000013 ffffffff c5b58ae0 c5893eb8 00000000 c5b58ae0 c57f6000 c02f3588
[ 3072.321470] 7d48  00000016 c03143d4 c5b58800 00000000 0000000d 00000001 00000000 0000000d
[ 3072.329650] 7d68  00000015 00000000 c52fb400 c57f7da8 c52fb400 c5b58c00 c5893eb8 c5b58ae0
[ 3072.337799] 7d88  c57f6000 c5b58aec 00000000 00000001 00000000 c02f55cc c5b58c00 c57f7da8
[ 3072.345948] 7da8  c52fb400 c57f7dfc 00000000 c5b58ae0 c57f6000 c5b58aec 00000000 00000001
[ 3072.354127] 7dc8  00000000 c02e3f34 c5b58a00 c5b58c00 c57b5d00 c5b58a00 c57b5d00 c02e406c
[ 3072.362276] 7de8  00000000 c5443420 c0077e8c c5b58aec c5b58aec c00ed348 c04279ec c57b5d00
[ 3072.370425] 7e08  c56886c8 00000000 c57cbf60 00000024 c0408210 c02d5c4c c56886c8 c57b5d00
[ 3072.378604]
[ 3072.378604] R4: 0xc5893e38:
[ 3072.382847] 3e38  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 3072.390996] 3e58  c5b58700 c5889800 c6112d80 c5888420 c5883b40 00000200 c5893e70 c5893e70
[ 3072.399175] 3e78  c02e9eec 00000000 00000000 00000000 c06a4b20 00000000 00000000 ffffffff
[ 3072.407324] 3e98  ffffffff 00000000 00000000 00000000 00000000 00000000 c5f9d600 00000000
[ 3072.415473] 3eb8  c587de08 c59e1a80 c5ba7b00 c58945bc c58937cc c587de10 c6005440 c05ea120
[ 3072.423652] 3ed8  c5b2ef00 00000002 00000003 00000000 00000000 00000001 c5893ef0 c5893ef0
[ 3072.431801] 3ef8  00000000 00000000 c5893f00 c5893f00 00000000 00000000 00000000 c589460c
[ 3072.439950] 3f18  c589381c 7fffffff c5893f20 c5893f20 00000000 00000000 00000000 00000000
[ 3072.448130]
[ 3072.448130] R6: 0xc5b58a60:
[ 3072.452372] 8a60  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 3072.460552] 8a80  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 3072.468700] 8aa0  00000000 00000000 00000000 c5b58a00 00000001 00000000 c5b58b00 c59e1ae0
[ 3072.476849] 8ac0  c59e1ba0 00000001 c5b58a00 00000001 00000001 c5b58c00 c59e1f60 c5ba1060
[ 3072.485029] 8ae0  00000000 c5b58ae4 c5b58ae4 c57f7df4 c57f7df4 c5893eb8 00000000 00000000
[ 3072.493178] 8b00  c5b58a00 c5b58aa8 00000000 00000000 64627573 63697665 30232065 00000000
[ 3072.501327] 8b20  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 3072.509506] 8b40  00000000 00000000 00000000 ffffffff 00000000 00000000 00000000 00000000
[ 3072.517655]
[ 3072.517655] R7: 0xc57f5f80:
[ 3072.521898] 5f80  00000000 00000004 c556f708 00000000 c57f5d80 01adad40 00000004 c57f5fa4
[ 3072.530077] 5fa0  00000000 656d616e 00000000 00000000 00000000 00000000 00000000 00000000
[ 3072.538226] 5fc0  00000000 00000000 00000000 00000000 c040b3e0 c590d600 00000000 c63ae540
[ 3072.546375] 5fe0  c57f5fe0 c57f5fe0 c5f442ac c00fb864 c57f5ff0 c57f5ff0 c57f5ff8 c57f5ff8
[ 3072.554554] 6000  00000000 00000002 00000000 c5443420 c05ccaac 00000000 00000015 c57f6000
[ 3072.562703] 6020  c5443420 c05cc100 c5a5ae60 c5a64600 c5b3e180 c05b8a18 c57f7c3c c57f7c10
[ 3072.570852] 6040  c03fa1f0 00000000 00000000 00000000 00000000 01000000 00000000 00000000
[ 3072.579032] 6060  4008c4c0 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 3072.587181]
[ 3072.587181] R10: 0xc06023dc:
[ 3072.591514] 23dc  00000014 0000000d 00000000 00000000 c0322f30 00000000 c0557357 c0554dc6
[ 3072.599694] 23fc  c0549b56 c04ed8f6 c0557372 c054dfc8 00000000 00000014 0000000f 00000000
[ 3072.607843] 241c  00000000 c0322f30 00000000 c0557383 c0554dec c0549b56 c04ed8f6 c055739e
[ 3072.615992] 243c  c054dfc8 00000000 00000014 0000000e 00000000 00000000 c0322f30 00000000
[ 3072.624171] 245c  c05573ee 00000000 00000000 c587de08 c5b36a00 00000000 c05fb9bc c05fb9bc
[ 3072.632320] 247c  00000001 c0602480 c0602480 00000001 c060248c c060248c 00000001 c0602498
[ 3072.640469] 249c  c0602498 00000001 c06024a4 c06024a4 00000001 00000000 00000000 00000000
[ 3072.648649] 24bc  00000000 00000000 00000000 00000000 00000000 00000000 00000000 c0601f14
[ 3072.656798] Process cat (pid: 616, stack limit = 0xc57f62e8)
[ 3072.662444] Stack: (0xc57f7d34 to 0xc57f8000)
[ 3072.666808] 7d20:                                                     c5893eb8 00000000 c5b58ae0
[ 3072.674957] 7d40: c57f6000 c02f3588 00000016 c03143d4 c5b58800 00000000 0000000d 00000001
```

```
[ 3072.683106] 7d60: 00000000 0000000d 00000015 00000000 c52fb400 c57f7da8 c52fb400 c5b58c00
[ 3072.691286] 7d80: c5893eb8 c5b58ae0 c57f6000 c5b58aec 00000000 00000001 00000000 c02f55cc
[ 3072.699435] 7da0: c5b58c00 c57f7da8 c52fb400 c57f7dfc 00000000 c5b58ae0 c57f6000 c5b58aec
[ 3072.707583] 7dc0: 00000000 00000001 00000000 c02e3f34 c5b58a00 c5b58c00 c57b5d00 c5b58a00
[ 3072.715763] 7de0: c57b5d00 c02e406c 00000000 c5443420 c0077e8c c5b58aec c5b58aec c00ed348
[ 3072.723912] 7e00: c04279ec c57b5d00 c56886c8 00000000 c57cbf60 00000024 c0408210 c02d5c4c
[ 3072.732091] 7e20: c56886c8 c57b5d00 c609edc0 00000000 00000000 c00edaf0 c56886c8 00000015
[ 3072.740240] 7e40: c600d8c0 c5fe3400 c57b5d00 c56886c8 c00ed924 c00e8ccc 00000000 c57f7ef8
[ 3072.748389] 7e60: c56886c8 00000000 00020000 00000000 c5edcd80 c00f6650 c5edcd80 c00e70f4
[ 3072.756569] 7e80: c06b77a0 c56886c8 c5448000 c57f7ef8 c57f7f78 c57f6000 c5372000 c0037fa8
[ 3072.764718] 7ea0: c57f6000 00000000 becbbc9c c00f69a8 c57f7ecc c07c76a0 c07c76ac c600d8c0
[ 3072.772867] 7ec0: c5fe3400 c5889800 c6112d80 00000000 c58937c0 c57f7f78 00000001 c5372000
[ 3072.781046] 7ee0: ffffff9c c0037fa8 00000000 c00f6d20 00000041 c08a0ba8 c600d8c0 c5fe3400
[ 3072.789195] 7f00: c4258677 00000008 c5372009 00000000 c5c6b400 c56886c8 00000101 00000004
[ 3072.797344] 7f20: 00000000 00000000 c5b36bac c02d5f58 c5b58700 c57b5a80 c5494a88 c5494a80
[ 3072.805523] 7f40: 00000000 00020000 00000003 00020001 00000000 00000000 ffffff9c 00000003
[ 3072.813672] 7f60: ffffff9c c5372000 00000001 c00e9a98 c5494a80 00000006 00020000 00000000
[ 3072.821821] 7f80: 00000024 00000100 c5494a80 becbbf12 ffffffff 00000001 00000005 c0037fa8
[ 3072.830001] 7fa0: 00000000 c0037e00 becbbf12 ffffffff becbbf12 00020000 00000000 00000000
[ 3072.838150] 7fc0: becbbf12 ffffffff 00000001 00000005 00000003 000dd760 0000008f becbbc9c
[ 3072.846299] 7fe0: 000fc350 becbb930 0000e9cc 47b8e824 60000010 becbbf12 4450536c 53204649
[ 3072.854509] [<c00e6988>] (kfree+0x5c/0xec) from [<c02f3588>] (dsp_add_new_paths+0x31c/0x35c)
[ 3072.862902] [<c02f3588>] (dsp_add_new_paths+0x31c/0x35c) from [<c02f55cc>] (soc_dsp_fe_dai_open
+0x30/0x1a8)
[ 3072.872638] [<c02f55cc>] (soc_dsp_fe_dai_open+0x30/0x1a8) from [<c02e3f34>] (snd_pcm_open_subst
ream+0x50/0x98)
[ 3072.882587] [<c02e3f34>] (snd_pcm_open_substream+0x50/0x98) from [<c02e406c>] (snd_pcm_open+0xf
0/0x1fc)
[ 3072.891988] [<c02e406c>] (snd_pcm_open+0xf0/0x1fc) from [<c02d5c4c>] (snd_open+0x174/0x240)
[ 3072.900320] [<c02d5c4c>] (snd_open+0x174/0x240) from [<c00edaf0>] (chrdev_open+0x1cc/0x1f0)
[ 3072.908652] [<c00edaf0>] (chrdev_open+0x1cc/0x1f0) from [<c00e8ccc>] (__dentry_open.isra.15+0x1
8c/0x298)
[ 3072.918113] [<c00e8ccc>] (__dentry_open.isra.15+0x18c/0x298) from [<c00f6650>] (do_last.isra.38
+0x524/0x678)
[ 3072.927910] [<c00f6650>] (do_last.isra.38+0x524/0x678) from [<c00f69a8>] (path_openat+0xb4/0x36
4)
[ 3072.936761] [<c00f69a8>] (path_openat+0xb4/0x364) from [<c00f6d20>] (do_filp_open+0x2c/0x78)
[ 3072.945185] [<c00f6d20>] (do_filp_open+0x2c/0x78) from [<c00e9a98>] (do_sys_open+0xd8/0x170)
[ 3072.953608] [<c00e9a98>] (do_sys_open+0xd8/0x170) from [<c0037e00>] (ret_fast_syscall+0x0/0x30)
[ 3072.962276] Code: 1a000006 e5913000 e3130903 1a000000 (e7f001f2)
[ 3072.976987] ---[ end trace cb7970f1a715b45a ]---
```