Alpine Linux - Bug #7047

v4l2-ctl segfaults when setting control values

03/22/2017 02:43 PM - Hannes Gustafsson

Status:	Closed	**Start date:**	03/22/2017
Priority:	Normal	**Due date:**	
Assignee:	Francesco Colista	**% Done:**	100%
Category:	Aports	**Estimated time:**	0.00 hour
Target version:	3.6.1		
Affected versions:	3.5.2	**Security IDs:**	

Description

Running Alpine in Docker on Ubuntu LTS segfaults

```
/ # v4l2-ctl -c exposure_auto=0
Segmentation fault (core dumped)
```

Several options fail too

```
/ # v4l2-ctl -c exposure_auto=0,white_balance_temperature_auto=1
Segmentation fault (core dumped)
```

Video device is mounted into container

```
docker run --device /dev/video0 -it alpine:3.5 /bin/sh
```

Getting camera info from within container works fine

```
/ # v4l2-ctl --all
Driver Info (not using libv4l2):
    Driver name   : uvcvideo
    Card type     : See3CAM_CU30
    Bus info      : usb-0000:00:14.0-2
    Driver version: 4.4.49
    Capabilities  : 0x84200001
        Video Capture
        Streaming
        Extended Pix Format
        Device Capabilities
    Device Caps   : 0x04200001
        Video Capture
        Streaming
        Extended Pix Format
Priority: 2
Video input : 0 (Camera 1: ok)
Format Video Capture:
    Width/Height      : 640/480
    Pixel Format      : 'UYVY'
    Field             : None
    Bytes per Line    : 1280
    Size Image        : 614400
    Colorspace        : Default
    Transfer Function : Default
    YCbCr Encoding    : Default
    Quantization      : Default
    Flags             :
Crop Capability Video Capture:
    Bounds      : Left 0, Top 0, Width 640, Height 480
    Default     : Left 0, Top 0, Width 640, Height 480
    Pixel Aspect: 1/1
Selection: crop_default, Left 0, Top 0, Width 640, Height 480
Selection: crop_bounds, Left 0, Top 0, Width 640, Height 480
```

```
Streaming Parameters Video Capture:
    Capabilities     : timeperframe
    Frames per second: 30.000 (30/1)
    Read buffers     : 0
                     brightness (int)    : min=-15 max=15 step=1 default=0 value=0
                       contrast (int)    : min=0 max=60 step=1 default=10 value=10
                     saturation (int)    : min=0 max=98 step=1 default=16 value=16
 white_balance_temperature_auto (bool)   : default=0 value=1
                          gamma (int)    : min=16 max=125 step=1 default=40 value=40
                           gain (int)    : min=0 max=100 step=1 default=0 value=1
      white_balance_temperature (int)    : min=11 max=50 step=1 default=17 value=17 flags=inactive
                      sharpness (int)    : min=1 max=7 step=1 default=1 value=1
                 exposure_auto (menu)    : min=0 max=3 default=1 value=0
             exposure_absolute (int)     : min=0 max=10000 step=1 default=312 value=312 flags=inac
tive
                  zoom_absolute (int)    : min=100 max=800 step=1 default=100 value=100
```

Trying to rebuild v4l-utils with debug info (DEBUG=1) and running in GDB yields the following backtrace:

```
(gdb) run -c exposure_auto=0
Starting program: /usr/bin/v4l2-ctl -c exposure_auto=0

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7dc0f2e in strchrnul () from /lib/ld-musl-x86_64.so.1
(gdb) bt
#0  0x00007ffff7dc0f2e in strchrnul () from /lib/ld-musl-x86_64.so.1
#1  0x000000000000003d in ?? ()
#2  0x00007ffff7dc0ed0 in strchr () from /lib/ld-musl-x86_64.so.1
#3  0x0000000000000000 in ?? ()
(gdb)
```

Other people have reported similar errors on IRC: http://dev.alpinelinux.org/irclogs/%23alpine-linux-2017-02.log

> 2017-02-02 15:20:50 <dnb_> Trying to run v4l2-ctl from v4l-utils, and it segfaults running any control operation... Wondering what the process should be to find out why? My devops guy tried compiling it on alpine, but having a hard time with musl and include paths, etc....

> 2017-02-02 22:01:33 <drewlover> v4l2-utils
> 2017-02-02 22:02:08 <drewlover> the package in alpine segfaults, and we don't have time to wait for upstream fixes, nor can we find out exactly wtf is going on with it... so... my devops guy is trying to build it himself, and failing miserably
> 2017-02-02 22:02:29 <Shiz> ah, right
> 2017-02-02 22:02:46 <Shiz> http://git.alpinelinux.org/cgit/aports/tree/main/v4l-utils?h=3.5-stable
> 2017-02-02 22:02:48 <drewlover> none of us have any understanding of musl and all that, and I haven't messed with C in like 10 years, so it's reallllly rusty to me
> 2017-02-02 22:02:54 <Shiz> well you can at least use the .patch here
> 2017-02-02 22:02:59 <Shiz> that should ostensibly make it compile
> 2017-02-02 22:04:30 <drewlover> I assume these are patches made simply to make it compile, but not tested for runtime
> 2017-02-02 22:05:16 <Shiz> well, usually the packages alpine ships are tested, but it should at least give you a base
> 2017-02-02 22:05:28 <Shiz> the patch isn't very special anyway, nothing that can induce a segfault
> 2017-02-02 22:06:06 <Shiz> that isnt /w 30

Versions:

```
# uname -a
Linux host 4.4.0-67-generic #88-Ubuntu SMP Wed Mar 8 16:34:45 UTC 2017 x86_64 x86_64 x86_64 GNU/Li
nux

docker version
Client:
 Version:      1.12.6
 API version:  1.24
 Go version:   go1.6.4
 Git commit:   78d1802
 Built:        Tue Jan 10 20:38:45 2017
```

```
 OS/Arch:      linux/amd64

Server:
 Version:      1.12.6
 API version:  1.24
 Go version:   go1.6.4
 Git commit:   78d1802
 Built:        Tue Jan 10 20:38:45 2017
 OS/Arch:      linux/amd64
```

Associated revisions

Revision bf732f20 - 05/31/2017 07:28 PM - Natanael Copa

main/v4l-utils: fix segfault due to undefined behavior in getsubopt

ref #7047

Revision dfa7d220 - 06/01/2017 08:15 AM - Natanael Copa

main/v4l-utils: fix segfault due to undefined behavior in getsubopt

fixes #7047

History

#1 - 03/24/2017 02:09 PM - Leonardo Arena

- Category set to Aports

- Assignee set to Francesco Colista

- Target version set to 3.6.0

#2 - 05/22/2017 01:58 PM - Carlo Landmeter

- Target version changed from 3.6.0 to 3.6.1

Seems this will not be resolved before 3.6. Moving target to 3.6.1

#3 - 05/31/2017 04:00 PM - Natanael Copa

this seems to be a bug (or feature?) in musl getsubopt

#4 - 05/31/2017 06:57 PM - Natanael Copa

problem explained here: http://www.openwall.com/lists/musl/2016/12/16/1

#5 - 06/01/2017 08:17 AM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset dfa7d220828b373c8d45ea627ea5b37dee28fcb7.

#6 - 06/01/2017 07:20 PM - Natanael Copa

- Status changed from Resolved to Closed