



author Alvin Šipraga <alsi@bang-olufsen.dk> 2023-03-02 17:36:47 +0100
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-04-05 11:15:37 +0200
commit 3256e152b645fc1e788ba44c2d8ced690113e3e6 (patch)
tree 7307f36a0661841b73b9b3534daf934b8afcc75f
parent b5ea8bc322c6c3bdf20c43b4a247420cfa63b7dd (diff)
download [linux-3256e152b645fc1e788ba44c2d8ced690113e3e6.tar.gz](#)

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

usb: gadget: u_audio: don't let userspace block driver unbind

commit 6c67ed9ad9b83e453e808f9b31a931a20a25629b upstream.

In the unbind callback for f_uac1 and f_uac2, a call to `snd_card_free()` via `g_audio_cleanup()` will disconnect the card and then wait for all resources to be released, which happens when the refcount falls to zero. Since userspace can keep the refcount incremented by not closing the relevant file descriptor, the call to unbind may block indefinitely. This can cause a deadlock during reboot, as evidenced by the following blocked task observed on my machine:

```
task:reboot state:D stack:0 pid:2827 ppid:569 flags:0x0000000c
Call trace:
```

```
__switch_to+0xc8/0x140
__schedule+0x2f0/0x7c0
schedule+0x60/0xd0
schedule_timeout+0x180/0x1d4
wait_for_completion+0x78/0x180
snd_card_free+0x90/0xa0
g_audio_cleanup+0x2c/0x64
afunc_unbind+0x28/0x60
...
kernel_restart+0x4c/0xac
__do_sys_reboot+0xcc/0x1ec
__arm64_sys_reboot+0x28/0x30
invoke_syscall+0x4c/0x110
...
```

The issue can also be observed by opening the card with `arecord` and then stopping the process through the shell before unbinding:

```
# arecord -D hw:UAC2Gadget -f S32_LE -c 2 -r 48000 /dev/null
Recording WAVE '/dev/null' : Signed 32 bit Little Endian, Rate 48000 Hz, Stereo
^Z[1]+  Stopped                  arecord -D hw:UAC2Gadget -f S32_LE -c 2 -r 48000 /dev/null
# echo gadget.0 > /sys/bus/gadget/drivers/configfs-gadget/unbind
(observer that the unbind command never finishes)
```

Fix the problem by using `snd_card_free_when_closed()` instead, which will still disconnect the card as desired, but defer the task of freeing the resources to the core once userspace closes its file descriptor.

Fixes: 132fcb460839 ("usb: gadget: Add Audio Class 2.0 Driver")

Cc: stable@vger.kernel.org
Signed-off-by: Alvin Šipraga <alsi@bang-olufsen.dk>
Reviewed-by: Ruslan Bilovol <ruslan.bilovol@gmail.com>
Reviewed-by: John Keeping <john@metanate.com>
Link: <https://lore.kernel.org/r/20230302163648.3349669-1-alvin@pqrs.dk>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

Diffstat

```
-rw-r--r-- drivers/usb/gadget/function/u_audio.c 2
```

1 files changed, 1 insertions, 1 deletions

```
diff --git a/drivers/usb/gadget/function/u_audio.c b/drivers/usb/gadget/function/u_audio.c
index 168303f21bf452..3136a239e78289 100644
--- a/drivers/usb/gadget/function/u_audio.c
+++ b/drivers/usb/gadget/function/u_audio.c
@@ -626,7 +626,7 @@ void g_audio_cleanup(struct g_audio *g_audio)
     uac = g_audio->uac;
     card = uac->card;
     if (card)
-        snd_card_free(card);
+        snd_card_free_when_closed(card);

     kfree(uac->p_prm.ureq);
     kfree(uac->c_prm.ureq);
```