



author Takashi Iwai <tiwai@suse.de> 2022-11-12 15:12:23 +0100
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-25 17:35:40 +0100
commit [872c9314769e89d8bda74ff3ac584756a45ee752](#) (patch)
tree [561be7bc27b3f0c706babfc8f7b51644bb9307d4](#)
parent [f2302d65e64f26ae22632c4a217a07f7cf3afe93](#) (diff)
download [linux-872c9314769e89d8bda74ff3ac584756a45ee752.tar.gz](#)

diff options

context:
space:
mode:

ALSA: usb-audio: Drop snd_BUG_ON() from snd_usbmidi_output_open()

commit ad72c3c3f6eb81d2cb189ec71e888316adada5df upstream.

snd_usbmidi_output_open() has a check of the NULL port with snd_BUG_ON(). snd_BUG_ON() was used as this shouldn't have happened, but in reality, the NULL port may be seen when the device gives an invalid endpoint setup at the descriptor, hence the driver skips the allocation. That is, the check itself is valid and snd_BUG_ON() should be dropped from there. Otherwise it's confusing as if it were a real bug, as recently syzbot stumbled on it.

Reported-by: syzbot+9abda841d636d86c41da@syzkaller.appspotmail.com

Cc: <stable@vger.kernel.org>

Link: <https://lore.kernel.org/r/syzbot+9abda841d636d86c41da@syzkaller.appspotmail.com>

Link: <https://lore.kernel.org/r/20221112141223.6144-1-tiwai@suse.de>

Signed-off-by: Takashi Iwai <tiwai@suse.de>

Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

Diffstat

```
-rw-r--r-- sound/usb/midi.c 4
```

1 files changed, 1 insertions, 3 deletions

diff --git a/sound/usb/midi.c b/sound/usb/midi.c

index 83da676519a8de..53d16b168df811 100644

--- a/sound/usb/midi.c

+++ b/sound/usb/midi.c

```
@@ -1148,10 +1148,8 @@ static int snd_usbmidi_output_open(struct snd_rawmidi_substream *substream)
                                port = &umidi->endpoints[i].out->ports[j];
                                break;
                                }
-       if (!port) {
-               snd_BUG();
+       if (!port)
+               return -ENXIO;
-       }

    substream->runtime->private_data = port;
    port->state = STATE_UNKNOWN;
```