author	Takashi Iwai <tiwai@suse.de>	2022-11-12 15:12:23 +0100
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-26 09:24:43 +0100
commit	02b94885b2fdf1808b1874e009bfb90753f8f4db (patch)	
tree	9ba134d941b7f1ff776cf1dd8525cd8818efaf96	
parent	7176d6f3adb92da6ceae607509e49dd929854f32 (diff)	
download	linux-02b94885b2fdf1808b1874e009bfb90753f8f4db.tar.gz	

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 344fbeadf161b0..9a361b202a09d9 100644
--- a/sound/usb/midi.c
+++ b/sound/usb/midi.c
@@ -1133,10 +1133,8 @@ 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;
```