author	Takashi Iwai <tiwai@suse.de>	2022-09-05 08:07:14 +0200
committer	Takashi Iwai <tiwai@suse.de>	2022-09-05 15:01:22 +0200
commit	8423f0b6d513b259fdab9c9bf4aaa6188d054c2d (patch)	
tree	5914cf974503f3799708d61372ef869a384be9f1	
parent	414d38ba871092aeac4ed097ac4ced89486646f7 (diff)	
download	linux-8423f0b6d513b259fdab9c9bf4aaa6188d054c2d.tar.gz	

diff options

context: 3

space: include

mode: unified

ALSA: pcm: oss: Fix race at SNDCTL_DSP_SYNC

```
There is a small race window at snd_pcm_oss_sync() that is called from
OSS PCM SNDCTL_DSP_SYNC ioctl; namely the function calls
snd_pcm_oss_make_ready() at first, then takes the params_lock mutex
for the rest.  When the stream is set up again by another thread
between them, it leads to inconsistency, and may result in unexpected
results such as NULL dereference of OSS buffer as a fuzzer spotted
recently.

The fix is simply to cover snd_pcm_oss_make_ready() call into the same
params_lock mutex with snd_pcm_oss_make_ready_locked() variant.

Reported-and-tested-by: butt3rflyh4ck <butterflyhuangxx@gmail.com>
Reviewed-by: Jaroslav Kysela <perex@perex.cz>
Cc: <stable@vger.kernel.org>
Link: https://lore.kernel.org/r/CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com
Link: https://lore.kernel.org/r/20220905060714.22549-1-tiwai@suse.de
Signed-off-by: Takashi Iwai <tiwai@suse.de>
```

Diffstat

-rw-r--r-- sound/core/oss/pcm_oss.c 6

1 files changed, 3 insertions, 3 deletions

```
diff --git a/sound/core/oss/pcm_oss.c b/sound/core/oss/pcm_oss.c
index 90c3a367d7de9..02df915eb3c66 100644
--- a/sound/core/oss/pcm_oss.c
+++ b/sound/core/oss/pcm_oss.c
@@ -1672,14 +1672,14 @@ static int snd_pcm_oss_sync(struct snd_pcm_oss_file *pcm_oss_file)
                runtime = substream->runtime;
                if (atomic_read(&substream->mmap_count))
                        goto __direct;
-               err = snd_pcm_oss_make_ready(substream);
-               if (err < 0)
-                       return err;
                atomic_inc(&runtime->oss.rw_ref);
                if (mutex_lock_interruptible(&runtime->oss.params_lock)) {
                        atomic_dec(&runtime->oss.rw_ref);
                        return -ERESTARTSYS;
                }
+               err = snd_pcm_oss_make_ready_locked(substream);
+               if (err < 0)
+                       goto unlock;
                format = snd_pcm_oss_format_from(runtime->oss.format);
                width = snd_pcm_format_physical_width(format);
                if (runtime->oss.buffer_used > 0) {
```