avcodec/g729postfilter: Fix undefined intermediate pointers

author Michael Niedermayer <michael@niedermayer.cc>
Fri, 27 Sep 2019 10:01:38 -0500 (17:01 +0200)
committer Michael Niedermayer <michael@niedermayer.cc>
Wed, 16 Oct 2019 12:17:57 -0500 (19:17 +0200)

Fixes: index -49 out of bounds for type 'int16_t [192]'
Fixes: 17689/clusterfuzz-testcase-minimized-ffmpeg_AV_CODEC_ID_ACELP_KELVIN_fuzzer-5756275014500352

Found-by: continuous fuzzing process https://github.com/google/oss-fuzz/tree/master/projects/ffmpeg
Signed-off-by: Michael Niedermayer <michael@niedermayer.cc>

libavcodec/g729postfilter.c patch | blob | history

diff --git a/libavcodec/g729postfilter.c b/libavcodec/g729postfilter.c

index e8e031a..ef4fec4 100644 (file)

```
--- a/libavcodec/g729postfilter.c
+++ b/libavcodec/g729postfilter.c
@@ -201,8 +201,8 @@ static int16_t long_term_filter(AudioDSPContext *adsp, int pitch_delay_int,
         }
         if (corr_int_num) {
             /* Compute denominator of pseudo-normalized correlation R'(0). */
-            corr_int_den = adsp->scalarproduct_int16(sig_scaled - best_delay_int + RES_PREV_DATA_SIZE,
-                                                     sig_scaled - best_delay_int + RES_PREV_DATA_SIZE,
+            corr_int_den = adsp->scalarproduct_int16(sig_scaled + RES_PREV_DATA_SIZE - best_delay_int,
+                                                     sig_scaled + RES_PREV_DATA_SIZE - best_delay_int,
                                                      subframe_size);

             /* Compute signals with non-integer delay k (with 1/8 precision),
```