Description

Integer Overflow in function lsr_translate_coords at
laser/lsr_dec.c:856

System info

Ubuntu 20.04 lts

Version info

```bash
git log
commit 68064e10172675e0853d6f429fb2055112835602 (HEAD -> master,
origin/master, origin/HEAD)
Author: jeanlf <jeanlf@gpac.io>
Date:   Fri Nov 18 10:36:10 2022 +0100

./MP4Box -version
MP4Box - GPAC version 2.1-DEV-rev490-g68064e101-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ -
http://gpac.io

Please cite our work in your research:
        GPAC Filters: https://doi.org/10.1145/3339825.3394929
        GPAC: https://doi.org/10.1145/1291233.1291452

GPAC Configuration: --enable-sanitizer --enable-debug
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SSL
GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_FAAD
GPAC_HAS_MAD GPAC_HAS_LIBA52 GPAC_HAS_JPEG GPAC_HAS_PNG
GPAC_HAS_FFMPEG GPAC_HAS_THEORA GPAC_HAS_VORBIS GPAC_HAS_XVID
GPAC_HAS_LINUX_DVB
```

compile

```bash
./configure --enable-sanitizer --enable-debug
make
```

crash command

```bash
MP4Box -bt poc
```

POC

[POC-Integer-Overflow]
(https://drive.google.com/file/d/170O0RtI03P1z4gE_ilRZQVS1w7uE7tX9/vi
ew?usp=sharing)

Occurrences:

[gpac/src/laser/lsr_dec.c:856:27]
(https://github.com/gpac/gpac/blob/68064e10172675e0853d6f429fb2055112
835602/src/laser/lsr_dec.c#L856)

```c
static Fixed lsr_translate_coords(GF_LASeRCodec *lsr, u32 val, u32
nb_bits)
{
        if (!nb_bits) return 0;

#ifdef GPAC_FIXED_POINT
        if (val >> (nb_bits-1) ) {
                s32 neg = (s32) val - (1<<nb_bits);
                if (neg < -FIX_ONE / 2)
                        return 2 * gf_divfix(INT2FIX(neg/2), lsr-
>res_factor);
                return gf_divfix(INT2FIX(neg), lsr->res_factor);
        } else {
                if (val > FIX_ONE / 2)
                        return 2 * gf_divfix(INT2FIX(val/2), lsr-
>res_factor);
                return gf_divfix(INT2FIX(val), lsr->res_factor);
        }
#else
        if (val >> (nb_bits-1) ) {
                s32 neg = (s32) val - (1<<nb_bits);
// <--- line:856
                return gf_divfix(INT2FIX(neg), lsr->res_factor);
        } else {
                return gf_divfix(INT2FIX(val), lsr->res_factor);
        }
#endif
}
```

Crash output

```bash
/home/zw/AFL_Fuzz_Datas/gpac-bt/bin/gcc/MP4Box -bt poc1
[iso file] extra box maxr found in hinf, deleting
[iso file] extra box maxr found in hinf, deleting
[iso file] Unknown box type 80rak in parent moov
[iso file] Unknown box type drzf in parent dinf
[iso file] Missing dref box in dinf
[iso file] Incomplete box mdat - start 11495 size 853090
[iso file] Incomplete file while reading for dump - aborting parsing
[iso file] extra box maxr found in hinf, deleting
[iso file] extra box maxr found in hinf, deleting
[iso file] Unknown box type 80rak in parent moov
[iso file] Unknown box type drzf in parent dinf
[iso file] Missing dref box in dinf
[iso file] Incomplete box mdat - start 11495 size 853090
[iso file] Incomplete file while reading for dump - aborting parsing
MPEG-4 LASeR Scene Parsing
[LASeR] sameg coded in bitstream but no g defined !
Reading 515 bits but max should be 64, skipping 451 most significants
bits
laser/lsr_dec.c:856:27: runtime error: left shift of 1 by 31 places
cannot be represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior
laser/lsr_dec.c:856:27 in
```