Integer Overflow in function lsr_translate_coords in gpac/gpac

0

Valid Reported on Jun 29th 2022

Description

Integer Overflow in function lsr_translate_coords at laser/lsr_dec.c:853

gpac version

```
git log
commit ea3af7c8242d1a82657dc3a518df5a5b1b5e27ed (HEAD -> master, origin/mas
Author: Romain Bouqueau <romain.bouqueau.pro@gmail.com>
Date:   Tue Jun 28 19:25:58 2022 +0200
```

POC

```
./MP4Box -bt ./poc_intof1_s.dat
laser/lsr_dec.c:853:10: runtime error: shift exponent 4294967295 is too lar
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior laser/lsr_dec.c:853
```

poc_intof1_s.dat

function lsr_translate_coords source code

```
static Fixed function lsr_translate_coords(GF_LASeRCodec *l
{
#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_factc
                return gf_divfix(INT2FIX(neg), lsr->res_factor);
        } else {
                if (val > FIX_ONE / 2)
                        return 2 * gf_divfix(INT2FIX(val/2), lsr->res_factc
                return gf_divfix(INT2FIX(val), lsr->res_factor);
        }
#else
        if (val >> (nb_bits-1) ) {    // <--- line:853
                s32 neg = (s32) val - (1<<nb_bits);
                return gf_divfix(INT2FIX(neg), lsr->res_factor);
        } else {
                return gf_divfix(INT2FIX(val), lsr->res_factor);
        }
#endif
}
```

GDB

```
gdb --args ./MP4Box -bt ./poc_intof1_s.dat

(gdb) b laser/lsr_dec.c:853
No source file named laser/lsr_dec.c.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 1 (laser/lsr_dec.c:853) pending.
(gdb) r
Starting program: /home/fuzz/fuzz/gpac/gpac/bin/gcc/MP4Box -bt ./poc_intof1
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, lsr_translate_coords (lsr=0x611000000540, val=0, nb_bits=0) a
853     laser/lsr_dec.c: No such file or directory.
(gdb) l
848     in laser/lsr dec.c
```

```
(gdb) p val
$1 = 0
(gdb) p (nb_bits-1)
$2 = 4294967295
(gdb) p nb_bits
$3 = 0
(gdb)
```

Impact

This vulnerability is capable of crashing software or use unexpected value.

CVE
CVE-2022-2454
(Published)

Vulnerability Type
CWE-190: Integer Overflow or Wraparound

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

TDHX ICS Security
@jieyongma
pro

We are processing your report and will contact the **gpac** team within 24 hours. 5 months ago

We have contacted a member of the **gpac** team and are waiting to hear back 5 months ago

A **gpac/gpac** maintainer 5 months ago Maintainer

https://github.com/gpac/gpac/issues/2213

We have sent a follow up to the **gpac** team. We will try again in 7 days. 5 months ago

We have sent a second follow up to the **gpac** team. We will try again in 10 days. 5 months ago

A **gpac/gpac** maintainer validated this vulnerability 4 months ago

TDHX ICS Security has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A **gpac/gpac** maintainer marked this as fixed in **2.1-DEV** with commit **faa75e** 4 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

TDHX 4 months ago Researcher

@admin can we get a CVE for this?

Jamie Slome 4 months ago Admin

@maintainer - are you happy for us to assign and publish a CVE? Once we get your permission, we can proceed with a CVE for this report 👍

A **gpac/gpac** maintainer 4 months ago

We agree. Please proceed with what's the best practice

We agree. Please proceed with what's the best practice.

Jamie Slome 4 months ago Admin

Done 👍

> Sign in to join this conversation