Use After Free in gpac/gpac

0

✓ Valid Reported on May 15th 2022

Description

Use After Free in gpac

Proof of Concept

```
MP4Box -bt POC1
```

POC1 is here

ASAN

```
==74043==ERROR: AddressSanitizer: heap-use-after-free on address 0x60400000
READ of size 8 at 0x604000003fd0 thread T0
    #0 0x7f0c5374e844 in gf_node_try_destroy /home/wjh/gpac/src/scenegraph/
    #1 0x7f0c537623c1 in gf_sg_command_del /home/wjh/gpac/src/scenegraph/co
    #2 0x7f0c53f10d1c in gf_sm_au_del /home/wjh/gpac/src/scene_manager/scen
    #3 0x7f0c53f0dcd8 in gf_sm_reset_stream /home/wjh/gpac/src/scene_manage
    #4 0x7f0c53f0dcd8 in gf_sm_delete_stream /home/wjh/gpac/src/scene_manag
    #5 0x7f0c53f0dcd8 in gf_sm_del /home/wjh/gpac/src/scene_manager/scene_m
    #6 0x505572 in dump_isom_scene /home/wjh/gpac/applications/mp4box/filed
    #7 0x4f3e66 in mp4box_main /home/wjh/gpac/applications/mp4box/mp4box.c:
    #8 0x7f0c52e34082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/c
    #9 0x42ac0d in _start (/home/wjh/gpac/bin/gcc/MP4Box+0x42ac0d)

0x604000003fd0 is located 0 bytes inside of 48-byte region [0x604000003fd0,
freed by thread T0 here:
    #0 0x4a49fd in free (/home/wjh/gpac/bin/gcc/MP4Box+0x4a49fd)
    #1 0x7f0c5374a1cf in gf_node_unregister /home/wjh/gpac/
    #2 0x7f0c5374e7dc in gf_node_try_destroy /home/wjh/gpac/src/scenegraph/
    #3 0x7f0c53f10d1c in gf_sm_au_del /home/wjh/gpac/src/scene_manager/scen
    #4 0x7f0c53f0dcd8 in gf_sm_reset_stream /home/wjh/gpac/src/scene_manage
    #5 0x7f0c53f0dcd8 in gf_sm_delete_stream /home/wjh/gpac/src/scene_manag

    #6 0x7f0c53f0dcd8 in gf_sm_del /home/wjh/gpac/src/scene_manager/scene_m

previously allocated by thread T0 here:
    #0 0x4a4c7d in malloc (/home/wjh/gpac/bin/gcc/MP4Box+0x4a4c7d)
    #1 0x7f0c5377e2db in Group_Create /home/wjh/gpac/src/scenegraph/mpeg4_n
    #2 0x7f0c5377e2db in gf_sg_mpeg4_node_new /home/wjh/gpac/src/scenegraph

SUMMARY: AddressSanitizer: heap-use-after-free /home/wjh/gpac/src/scenegrap
Shadow bytes around the buggy address:
  0x0c087fff87a0: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
  0x0c087fff87b0: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
  0x0c087fff87c0: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
  0x0c087fff87d0: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
  0x0c087fff87e0: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
=>0x0c087fff87f0: fa fa 00 00 00 00 02 fa fa fa[fd]fd fd fd fd fd
  0x0c087fff8800: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fa
  0x0c087fff8810: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fa
  0x0c087fff8820: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c087fff8830: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c087fff8840: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc

==74043==ABORTING
```

Impact

can cause a program to crash, use unexpected values, or execute code.

CVE
CVE-2022-1795
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.3)

Registry
Other

Affected Version
2.1-DEV

Visibility
Public

Status
Fixed

Found by

wjhwjhn
@wjhwjhn
unranked

This report was seen 635 times.

Chat with us

We are processing your report and will contact the gpac team within 24 hours. 6 months ago

We have contacted a member of the **gpac** team and are waiting to hear back 6 months ago

A **gpac/gpac** maintainer validated this vulnerability 6 months ago

wjhwjhn 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 **v2.1.0-DEV** with commit **c535ba** 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

wjhwjhn 6 months ago Researcher

Hi @admin, may i have CVE assigned to this case? Thanks!

Jamie Slome 6 months ago Admin

Sorted 👍

Sign in to join this conversation

huntr

home

part of 418sec

company

Chat with us

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

about

team

Chat with us