Heap Use After Free in function Q_IsTypeOn in gpac/gpac

0

Valid Reported on Jun 29th 2022

Description

Heap Use After Free in function Q_IsTypeOn at src/bifs/unquantize.c:169

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_huaf1_s.dat

=================================================================
==1301527==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000
READ of size 4 at 0x6100000023c4 thread T0
    #0 0x7ffff2264f87 in Q_IsTypeOn /home/fuzz/fuzz/gpac/src/bifs/unquantiz
    #1 0x7ffff2273d98 in gf_bifs_dec_unquant_field /home/fuzz/fuzz/gpac/src
    #2 0x7ffff21ab00d in gf_bifs_dec_sf_field /home/fuzz/fuzz/gpac/src/bifs
    #3 0x7ffff21bf41f in gf_bifs_dec_field /home/fuzz/fuzz/gpac/src/bifs/fi
    #4 0x7ffff21c2403 in gf_bifs_dec_node_mask /home/fuzz/fuzz/gpac/src/bif
    #5 0x7ffff21b9791 in gf_bifs_dec_node /home/fuzz/fuzz/gpac/src/bifs/fie
    #6 0x7ffff21bd7c3 in BD_DecMFFieldVec /home/fuzz/fuzz/gpac/src/bifs/fie
    #7 0x7ffff21c064f in gf_bifs_dec_field /home/fuzz/fuzz/gpac/src/bifs/fi
    #8 0x7ffff21c18e5 in gf_bifs_dec_node_list /home/fuzz/f
    #9 0x7ffff21b984b in gf_bifs_dec_node /home/fuzz/fuzz/gp
    #10 0x7ffff21dd60c in BM_ParseNodeInsert /home/fuzz/fuzz/gpac/src/bifs/
```

```
    #11 0x7ffff21e24d3 in BM_ParseInsert /home/fuzz/fuzz/gpac/src/bifs/memc
    #12 0x7ffff21eeb02 in BM_ParseCommand /home/fuzz/fuzz/gpac/src/bifs/mem
    #13 0x7ffff21f05d2 in gf_bifs_flush_command_list /home/fuzz/fuzz/gpac/s
    #14 0x7ffff21f32bc in gf_bifs_decode_command_list /home/fuzz/fuzz/gpac/
    #15 0x7ffff39a4274 in gf_sm_load_run_isom /home/fuzz/fuzz/gpac/src/scer
    #16 0x7ffff3844fee in gf_sm_load_run /home/fuzz/fuzz/gpac/src/scene_mar
    #17 0x585735 in dump_isom_scene /home/fuzz/fuzz/gpac/applications/mp4bc
    #18 0x54321e in mp4box_main /home/fuzz/fuzz/gpac/applications/mp4box/mp
    #19 0x553f31 in main /home/fuzz/fuzz/gpac/applications/mp4box/mp4box.c:
    #20 0x7fffeee04082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #21 0x42abed in _start (/home/fuzz/fuzz/gpac/gpac/bin/gcc/MP4Box+0x42ab

0x6100000023c4 is located 132 bytes inside of 192-byte region [0x610000002
freed by thread T0 here:
    #0 0x4a5be2 in free (/home/fuzz/fuzz/gpac/gpac/bin/gcc/MP4Box+0x4a5be2)
    #1 0x7ffff0d72324 in gf_free /home/fuzz/fuzz/gpac/src/utils/alloc.c:165
    #2 0x7ffff128e631 in gf_node_free /home/fuzz/fuzz/gpac/src/scenegraph/b
    #3 0x7ffff13bda9c in QuantizationParameter_Del /home/fuzz/fuzz/gpac/src
    #4 0x7ffff13afa2d in gf_sg_mpeg4_node_del /home/fuzz/fuzz/gpac/src/scer
    #5 0x7ffff1272b50 in gf_node_del /home/fuzz/fuzz/gpac/src/scenegraph/ba
    #6 0x7ffff12610b9 in gf_node_unregister /home/fuzz/fuzz/gpac/src/sceneg
    #7 0x7ffff12853d4 in gf_node_unregister_children /home/fuzz/fuzz/gpac/s
    #8 0x7ffff13bb3f5 in LOD_Del /home/fuzz/fuzz/gpac/src/scenegraph/mpeg4_
    #9 0x7ffff13af45d in gf_sg_mpeg4_node_del /home/fuzz/fuzz/gpac/src/scer
    #10 0x7ffff1272b50 in gf_node_del /home/fuzz/fuzz/gpac/src/scenegraph/b
    #11 0x7ffff12610b9 in gf_node_unregister /home/fuzz/fuzz/gpac/src/scene
    #12 0x7ffff21b9b8c in gf_bifs_dec_node /home/fuzz/fuzz/gpac/src/bifs/fi
    #13 0x7ffff21dd60c in BM_ParseNodeInsert /home/fuzz/fuzz/gpac/src/bifs/
    #14 0x7ffff21e24d3 in BM_ParseInsert /home/fuzz/fuzz/gpac/src/bifs/memc
    #15 0x7ffff21eeb02 in BM_ParseCommand /home/fuzz/fuzz/gpac/src/bifs/mem
    #16 0x7ffff21f05d2 in gf_bifs_flush_command_list /home/fuzz/fuzz/gpac/s
    #17 0x7ffff21f32bc in gf_bifs_decode_command_list /home/fuzz/fuzz/gpac/
    #18 0x7ffff39a4274 in gf_sm_load_run_isom /home/fuzz/fuzz/gpac/src/scer
    #19 0x7ffff3844fee in gf_sm_load_run /home/fuzz/fuzz/gpac/src/scene_mar
    #20 0x585735 in dump_isom_scene /home/fuzz/fuzz/gpac/applications/mp4bc
    #21 0x54321e in mp4box_main /home/fuzz/fuzz/gpac/applications/mp4box/mp
    #22 0x553f31 in main /home/fuzz/fuzz/gpac/applications/mp4box/mp4box.c:
    #23 0x7fffeee04082 in __libc_start_main /build/glibc-SzI

previously allocated by thread T0 here:
```

```
    #0 0x4a5e4d in malloc (/home/fuzz/fuzz/gpac/gpac/bin/gcc/MP4Box+0x4a5e4
    #1 0x7ffff0d72214 in gf_malloc /home/fuzz/fuzz/gpac/src/utils/alloc.c:1
    #2 0x7ffff132e244 in QuantizationParameter_Create /home/fuzz/fuzz/gpac/

    #3 0x7ffff13a96f6 in gf_sg_mpeg4_node_new /home/fuzz/fuzz/gpac/src/scer
    #4 0x7ffff1298209 in gf_node_new /home/fuzz/fuzz/gpac/src/scenegraph/ba
    #5 0x7ffff21b91b4 in gf_bifs_dec_node /home/fuzz/fuzz/gpac/src/bifs/fie
    #6 0x7ffff21bd7c3 in BD_DecMFFieldVec /home/fuzz/fuzz/gpac/src/bifs/fie
    #7 0x7ffff21c064f in gf_bifs_dec_field /home/fuzz/fuzz/gpac/src/bifs/fi
    #8 0x7ffff21c18e5 in gf_bifs_dec_node_list /home/fuzz/fuzz/gpac/src/bif
    #9 0x7ffff21b984b in gf_bifs_dec_node /home/fuzz/fuzz/gpac/src/bifs/fie
    #10 0x7ffff21dd60c in BM_ParseNodeInsert /home/fuzz/fuzz/gpac/src/bifs/
    #11 0x7ffff21e24d3 in BM_ParseInsert /home/fuzz/fuzz/gpac/src/bifs/memc
    #12 0x7ffff21eeb02 in BM_ParseCommand /home/fuzz/fuzz/gpac/src/bifs/mem
    #13 0x7ffff21f05d2 in gf_bifs_flush_command_list /home/fuzz/fuzz/gpac/s
    #14 0x7ffff21f32bc in gf_bifs_decode_command_list /home/fuzz/fuzz/gpac/
    #15 0x7ffff39a4274 in gf_sm_load_run_isom /home/fuzz/fuzz/gpac/src/scer
    #16 0x7ffff3844fee in gf_sm_load_run /home/fuzz/fuzz/gpac/src/scene_mar
    #17 0x585735 in dump_isom_scene /home/fuzz/fuzz/gpac/applications/mp4bc
    #18 0x54321e in mp4box_main /home/fuzz/fuzz/gpac/applications/mp4box/mp
    #19 0x553f31 in main /home/fuzz/fuzz/gpac/applications/mp4box/mp4box.c:
    #20 0x7fffeee04082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/fuzz/gpac/src/bit
Shadow bytes around the buggy address:
  0x0c207fff8420: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fff8430: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c207fff8440: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fff8450: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c207fff8460: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff8470: fd fd fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd
  0x0c207fff8480: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fff8490: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fff84a0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fff84b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fff84c0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
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:     ca
    Right alloca redzone:    cb
    Shadow gap:              cc
==1301527==ABORTING
```

poc_huaf1_s.dat

Impact

This vulnerability is capable of crashing software, use unexpected value, or possible code execution.

CVE
CVE-2022-2453
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility

Public

Status
Fixed

Found by

TDHX ICS Security
@jieyongma
pro

This report was seen 481 times.

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/2212

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 **dc7de8** 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 Maintainer

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

Jamie Slome 4 months ago Admin

Done 👍

Sign in to join this conversation