Use After Free in gpac/gpac

Valid Reported on Jan 20th 2022

0

Description

Use After Free in gpac

Proof of Concept

```
MP4Box -bt POC4
MP4Box -bt POC5
```

POC4 is here. POC5 is here.

ASAN

```
==414586==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000(
READ of size 4 at 0x6100000007fc thread T0
    #0 0x7f792608124f in BD_ReadSFFloat bifs/field_decode.c:68
    #1 0x7f792608124f in gf_bifs_dec_sf_field bifs/field_decode.c:112
    #2 0x7f79260835ca in gf_bifs_dec_node_mask bifs/field_decode.c:656
    #3 0x7f792607d212 in gf_bifs_dec_node bifs/field_decode.c:918
    #4 0x7f7926068f24 in gf_bifs_dec_proto_list bifs/com_dec.c:1143
    #5 0x7f7926068eff in gf_bifs_dec_proto_list bifs/com_dec.c:1132
    #6 0x7f7926069790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #7 0x7f792609318a in BM_SceneReplace bifs/memory_decoder.c:860
    #8 0x7f7926093b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #9 0x7f79260946fc in gf_bifs_decode_command_list bifs/memory_decoder.c:
    #10 0x7f7926631eac in gf_sm_load_run_isom scene_manager/loader_isom.c:3
    #11 0x556d347e807b in dump_isom_scene /home/zxq/CVE_testing/ASAN-instal
    #12 0x556d347d2d60 in mp4boxMain /home/zxq/CVE_testing/ASAN-install/gpac
    #13 0x7f79236610b2 in __libc_start_main (/lib/x86_64-li
    #14 0x556d347aeb1d in _start (/home/zxq/CVE_testing/ASAN-install/gpac/b
```

```
0x6100000007fc is located 188 bytes inside of 192-byte region [0x610000000
freed by thread T0 here:

    #0 0x7f792974d7cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.
    #1 0x7f7925d2df6d in gf_node_unregister scenegraph/base_scenegraph.c:76
    #2 0x7f7925d2eb05 in gf_node_unregister_children scenegraph/base_sceneg
    #3 0x7f7925ee916e in gf_sg_vrml_parent_destroy scenegraph/vrml_tools.c:
    #4 0x7f7925dfdedd in TemporalTransform_Del scenegraph/mpeg4_nodes.c:222
    #5 0x7f7925dfdedd in gf_sg_mpeg4_node_del scenegraph/mpeg4_nodes.c:3785
    #6 0x7f7925d2df6d in gf_node_unregister scenegraph/base_scenegraph.c:76
    #7 0x7f792607de2f in gf_bifs_dec_node bifs/field_decode.c:930
    #8 0x7f7926068f24 in gf_bifs_dec_proto_list bifs/com_dec.c:1143
    #9 0x7f7926069790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #10 0x7f792609318a in BM_SceneReplace bifs/memory_decoder.c:860
    #11 0x7f7926093b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #12 0x7f7926093e69 in gf_bifs_flush_command_list bifs/memory_decoder.c:
    #13 0x7f7926068f4a in gf_bifs_dec_proto_list bifs/com_dec.c:1162
    #14 0x7f7926068eff in gf_bifs_dec_proto_list bifs/com_dec.c:1132
    #15 0x7f7926069790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #16 0x7f792609318a in BM_SceneReplace bifs/memory_decoder.c:860
    #17 0x7f7926093b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #18 0x7f79260946fc in gf_bifs_decode_command_list bifs/memory_decoder.c
    #19 0x7f7926631eac in gf_sm_load_run_isom scene_manager/loader_isom.c:3
    #20 0x556d347e807b in dump_isom_scene /home/zxq/CVE_testing/ASAN-instal
    #21 0x556d347d2d60 in mp4boxMain /home/zxq/CVE_testing/ASAN-install/gpa
    #22 0x7f79236610b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

previously allocated by thread T0 here:
    #0 0x7f792974dbc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc
    #1 0x7f7925ddc107 in QuantizationParameter_Create scenegraph/mpeg4_node
    #2 0x7f7925d2fe86 in gf_node_new scenegraph/base_scenegraph.c:1994
    #3 0x7f792607d185 in gf_bifs_dec_node bifs/field_decode.c:892
    #4 0x7f79260824a1 in BD_DecMFFieldVec bifs/field_decode.c:432
    #5 0x7f7926082b2d in gf_bifs_dec_field bifs/field_decode.c:558
    #6 0x7f7926083035 in gf_bifs_dec_node_list bifs/field_decode.c:618
    #7 0x7f792607cfd4 in gf_bifs_dec_node bifs/field_decode.c:920
    #8 0x7f7926068f24 in gf_bifs_dec_proto_list bifs/com_dec.c:1143
    #9 0x7f7926069790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #10 0x7f792609318a in BM_SceneReplace bifs/memory_decod
    #11 0x7f7926093b6e in BM_ParseCommand bifs/memory_decoder.c:910
```

```
    #12 0x7f7926093e69 in gf_bifs_flush_command_list bifs/memory_decoder.c:
    #13 0x7f7926068f4a in gf_bifs_dec_proto_list bifs/com_dec.c:1162
    #14 0x7f7926068eff in gf_bifs_dec_proto_list bifs/com_dec.c:1132

    #15 0x7f7926069790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #16 0x7f792609318a in BM_SceneReplace bifs/memory_decoder.c:860
    #17 0x7f7926093b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #18 0x7f79260946fc in gf_bifs_decode_command_list bifs/memory_decoder.c
    #19 0x7f7926631eac in gf_sm_load_run_isom scene_manager/loader_isom.c:3
    #20 0x556d347e807b in dump_isom_scene /home/zxq/CVE_testing/ASAN-instal
    #21 0x556d347d2d60 in mp4boxMain /home/zxq/CVE_testing/ASAN-install/gpa
    #22 0x7f79236610b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

SUMMARY: AddressSanitizer: heap-use-after-free bifs/field_decode.c:68 in BD
Shadow bytes around the buggy address:
  0x0c207fff80a0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fff80b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fff80c0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fff80d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fff80e0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff80f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]
  0x0c207fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 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:     ca

  Right alloca redzone:    cb
  Shadow gap:              cc
==414586==ABORTING
```

```
==1293588==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000
READ of size 4 at 0x6100000004e4 thread T0
    #0 0x7f13db4147f7 in Q_IsTypeOn bifs/unquantize.c:185
    #1 0x7f13db41a3f4 in gf_bifs_dec_unquant_field bifs/unquantize.c:397
    #2 0x7f13db3e3b4a in gf_bifs_dec_sf_field bifs/field_decode.c:84
    #3 0x7f13db3e767f in BD_DecMFFieldVec bifs/field_decode.c:426
    #4 0x7f13db3e7b2d in gf_bifs_dec_field bifs/field_decode.c:558
    #5 0x7f13db3e8035 in gf_bifs_dec_node_list bifs/field_decode.c:618
    #6 0x7f13db3e1fd4 in gf_bifs_dec_node bifs/field_decode.c:920
    #7 0x7f13db3cdf24 in gf_bifs_dec_proto_list bifs/com_dec.c:1143
    #8 0x7f13db3ce790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #9 0x7f13db3f818a in BM_SceneReplace bifs/memory_decoder.c:860
    #10 0x7f13db3f8b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #11 0x7f13db3f96fc in gf_bifs_decode_command_list bifs/memory_decoder.c
    #12 0x7f13db996eac in gf_sm_load_run_isom scene_manager/loader_isom.c:3
    #13 0x56255741007b in dump_isom_scene /home/zxq/CVE_testing/ASAN-instal
    #14 0x5625573fad60 in mp4boxMain /home/zxq/CVE_testing/ASAN-install/gpa
    #15 0x7f13d89c60b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #16 0x5625573d6b1d in _start (/home/zxq/CVE_testing/ASAN-install/gpac/b

0x6100000004e4 is located 164 bytes inside of 192-byte region [0x610000000
freed by thread T0 here:
    #0 0x7f13deab27cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.
    #1 0x7f13db092f6d in gf_node_unregister scenegraph/base_scenegraph.c:76
    #2 0x7f13db093b05 in gf_node_unregister_children scenegraph/base_sceneg
    #3 0x7f13db24e16e in gf_sg_vrml_parent_destroy scenegraph/vrml_tools.c:
    #4 0x7f13db162edd in TemporalTransform_Del scenegraph/mpeg4_nodes.c:222
    #5 0x7f13db162edd in gf_sg_mpeg4_node_del scenegraph/mp
    #6 0x7f13db092f6d in gf_node_unregister scenegraph/base_
    #7 0x7f13db3e2e2f in gf_bifs_dec_node bifs/field_decode.c:930
```

```
    #8 0x7f13db3cdf24 in gf_bifs_dec_proto_list bifs/com_dec.c:1143
    #9 0x7f13db3ce790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #10 0x7f13db3f818a in BM_SceneReplace bifs/memory_decoder.c:860

    #11 0x7f13db3f8b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #12 0x7f13db3f8e69 in gf_bifs_flush_command_list bifs/memory_decoder.c
    #13 0x7f13db3cdf4a in gf_bifs_dec_proto_list bifs/com_dec.c:1162
    #14 0x7f13db3cdeff in gf_bifs_dec_proto_list bifs/com_dec.c:1132
    #15 0x7f13db3ce790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #16 0x7f13db3f818a in BM_SceneReplace bifs/memory_decoder.c:860
    #17 0x7f13db3f8b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #18 0x7f13db3f96fc in gf_bifs_decode_command_list bifs/memory_decoder.c
    #19 0x7f13db996eac in gf_sm_load_run_isom scene_manager/loader_isom.c:3
    #20 0x56255741007b in dump_isom_scene /home/zxq/CVE_testing/ASAN-instal
    #21 0x5625573fad60 in mp4boxMain /home/zxq/CVE_testing/ASAN-install/gpa
    #22 0x7f13d89c60b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

previously allocated by thread T0 here:
    #0 0x7f13deab2bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc
    #1 0x7f13db141107 in QuantizationParameter_Create scenegraph/mpeg4_node
    #2 0x7f13db094e86 in gf_node_new scenegraph/base_scenegraph.c:1994
    #3 0x7f13db3e2185 in gf_bifs_dec_node bifs/field_decode.c:892
    #4 0x7f13db3e74a1 in BD_DecMFFieldVec bifs/field_decode.c:432
    #5 0x7f13db3e7b2d in gf_bifs_dec_field bifs/field_decode.c:558
    #6 0x7f13db3e8035 in gf_bifs_dec_node_list bifs/field_decode.c:618
    #7 0x7f13db3e1fd4 in gf_bifs_dec_node bifs/field_decode.c:920
    #8 0x7f13db3cdf24 in gf_bifs_dec_proto_list bifs/com_dec.c:1143
    #9 0x7f13db3ce790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #10 0x7f13db3f818a in BM_SceneReplace bifs/memory_decoder.c:860
    #11 0x7f13db3f8b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #12 0x7f13db3f8e69 in gf_bifs_flush_command_list bifs/memory_decoder.c
    #13 0x7f13db3cdf4a in gf_bifs_dec_proto_list bifs/com_dec.c:1162
    #14 0x7f13db3cdeff in gf_bifs_dec_proto_list bifs/com_dec.c:1132
    #15 0x7f13db3ce790 in BD_DecSceneReplace bifs/com_dec.c:1351
    #16 0x7f13db3f818a in BM_SceneReplace bifs/memory_decoder.c:860
    #17 0x7f13db3f8b6e in BM_ParseCommand bifs/memory_decoder.c:910
    #18 0x7f13db3f96fc in gf_bifs_decode_command_list bifs/memory_decoder.c
    #19 0x7f13db996eac in gf_sm_load_run_isom scene_manager/loader_isom.c:3
    #20 0x56255741007b in dump_isom_scene /home/zxq/CVE_testing/ASAN-instal
    #21 0x5625573fad60 in mp4boxMain /home/zxq/CVE_testing/
    #22 0x7f13d89c60b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
```

```
SUMMARY: AddressSanitizer: heap-use-after-free bifs/unquantize.c:185 in Q_]
Shadow bytes around the buggy address:

  0x0c207fff8040: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05
  0x0c207fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff8080: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff8090: fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd fd fd
  0x0c207fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 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:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==1293588==ABORTING
```

Vulnerability Type
CWE-416: Use After Free

Severity

Medium (5.5)

Visibility
Public

Status
Fixed

Found by

zfeixq

@zfeixq

unranked

This report was seen 472 times.

We are processing your report and will contact the **gpac** team within 24 hours. 10 months ago

zfeixq modified the report 10 months ago

We have contacted a member of the **gpac** team and are waiting to hear back 10 months ago

A **gpac/gpac** maintainer 10 months ago Maintainer

cf https://github.com/gpac/gpac/issues/2061

A **gpac/gpac** maintainer validated this vulnerability 10 months ago

zfeixq has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **gpac/gpac** maintainer marked this as fixed in **1.1.0** with commit **96699a** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation