Stack-based Buffer Overflow in gpac/gpac

0

Valid Reported on Jan 20th 2022

Description

Stack-based Buffer Overflow in gpac

Proof of Concept

```
MP4Box -bt POC3
```

POC3is here

gdb

```
Program received signal SIGABRT, Aborted.
0x0000000000b68d4b in raise ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
─────────────────────────────────────────────────────────────────────────────────
 RAX  0x0
 RBX  0xf1e8c0 ◂— 0xf1e8c0
 RCX  0xb68d4b (raise+203) ◂— mov    rax, qword ptr [rsp + 0x108]
 RDX  0x0
 RDI  0x2
 RSI  0x7fffffff53a0 ◂— 0x0
 R8   0x0
 R9   0x7fffffff53a0 ◂— 0x0
 R10  0x8
 R11  0x246
 R12  0x7fffffff5620 —▸ 0x7fffffff8260 ◂— 0x2fffffffc
 R13  0x20
 R14  0x7ffff7ff8000 ◂— 0x202a2a2a00001000
 R15  0x1
```

```
RBP  0x7fffffff5720 —▸ 0xdd9047 ◂— '*** %s ***: terminated\n'
RSP  0x7fffffff53a0 ◂— 0x0
RIP  0xb68d4b (raise+203) ◂— mov    rax, qword ptr [rsp + 0x108]
```

```
► 0xb68d4b <raise+203>         mov    rax, qword ptr [rsp + 0x108]
  0xb68d53 <raise+211>         xor    rax, qword ptr fs:[0x28]
  0xb68d5c <raise+220>         jne    raise+260                     <rais
   ↓
  0xb68d84 <raise+260>         call   __stack_chk_fail_local

  0xb68d89                     nop    dword ptr [rax]
  0xb68d90 <sigprocmask>       endbr64
  0xb68d94 <sigprocmask+4>     sub    rsp, 0x98
  0xb68d9b <sigprocmask+11>    xor    r8d, r8d
  0xb68d9e <sigprocmask+14>    mov    rax, qword ptr fs:[0x28]
  0xb68da7 <sigprocmask+23>    mov    qword ptr [rsp + 0x88], rax
  0xb68daf <sigprocmask+31>    xor    eax, eax
```

```
00:0000| rsi r9 rsp 0x7fffffff53a0 ◂— 0x0
... ↓              2 skipped
03:0018|           0x7fffffff53b8 ◂— 0x9c43be786800fa00
04:0020|           0x7fffffff53c0 ◂— 0x0
05:0028|           0x7fffffff53c8 ◂— 0x9c43be786800fa00
06:0030|           0x7fffffff53d0 —▸ 0x7fffffff5430 ◂— 0xffffffffffffffff
07:0038|           0x7fffffff53d8 —▸ 0xf0e060 (_IO_file_jumps) ◂— 0x0
```

```
► f 0         0xb68d4b raise+203
  f 1         0x401f71 abort+299
  f 2         0xb80486 __libc_message+662
  f 3         0xbd5f0a __fortify_fail+42
  f 4         0xbd5ed6
  f 5         0x50fe96
  f 6         0x51010d gf_bifs_dec_unquant_field+621
  f 7         0x4fd668 gf_bifs_dec_sf_field+56
```

```
pwndbg> bt
#0  0x0000000000b68d4b in raise ()
#1  0x0000000000401f71 in abort ()
#2  0x0000000000b80486 in __libc_message ()
#3  0x0000000000bd5f0a in __fortify_fail ()
```

```
#4  0x00000000000bd5ed6 in __stack_chk_fail_local ()
#5  0x000000000050fe96 in Q_DecNormal ()
#6  0x000000000051010d in gf_bifs_dec_unquant_field ()

#7  0x00000000004fd668 in gf_bifs_dec_sf_field ()
#8  0x00000000004fea3d in gf_bifs_dec_node_list ()
#9  0x00000000004fd176 in gf_bifs_dec_node ()
#10 0x00000000004fe5ac in BD_DecMFFieldVec ()
#11 0x00000000004fe80b in gf_bifs_dec_field.part ()
#12 0x00000000004fe9e7 in gf_bifs_dec_node_list ()
#13 0x00000000004fd176 in gf_bifs_dec_node ()
#14 0x00000000004f540d in gf_bifs_dec_proto_list ()
#15 0x00000000004f56e9 in BD_DecSceneReplace ()
#16 0x000000000050405e in BM_SceneReplace ()
#17 0x000000000050424f in BM_ParseCommand ()
#18 0x0000000000504344 in gf_bifs_flush_command_list ()
#19 0x00000000004f5433 in gf_bifs_dec_proto_list ()
#20 0x00000000004f53ec in gf_bifs_dec_proto_list ()
#21 0x00000000004f56e9 in BD_DecSceneReplace ()
#22 0x000000000050405e in BM_SceneReplace ()
#23 0x000000000050424f in BM_ParseCommand ()
#24 0x00000000005045c1 in gf_bifs_decode_command_list ()
#25 0x0000000000628df1 in gf_sm_load_run_isom ()
#26 0x000000000041bd58 in dump_isom_scene ()
#27 0x00000000004125ec in mp4boxMain ()
#28 0x0000000000b599e0 in __libc_start_main ()
#29 0x0000000000402cbe in _start ()
```

Vulnerability Type
CWE-121: Stack-based Buffer Overflow

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

zfeixq

@zfeixq

unranked

This report was seen 477 times.

We are processing your report and will contact the **gpac** team within 24 hours. 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/2058

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 **b13e99** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation