

## NULL Pointer Dereference in gpac/gpac

0



Reported on Jan 18th 2022

### Description

Null Pointer Dereference in gf\_dump\_vrml\_field.isra ()

### Proof of Concept

MP4Box -bt POC2

POC2 is here.

### Bt

Program received signal SIGSEGV, Segmentation fault.

0x0000000000644ca4 in gf\_dump\_vrml\_field.isra ()

LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

[ F

RAX 0x1

RBX 0x1

RCX 0x0

RDX 0x0

RDI 0xf3a100 ← 0x0

RSI 0xc6a6e6 ← 0x7365445f5345005b /\* '[' \*/

R8 0x1

R9 0x1

R10 0xffffffff9

R11 0xf392a0 ← 0x30646c6569665f /\* '\_field0' \*/

R12 0x0

R13 0xf38710 → 0xf2d950 ← 0x0

R14 0x0

R15 0x3b

RIP 0x5200000000000000 0x5200000000000000 0x1000100000000000

Chat with us

```

RBP 0x139960 → 0x1399b0 ← 0x100010001
RSP 0x7fffffff70c0 → 0xf392a0 ← 0x30646c6569665f /* '_field0' */
RIP 0x644ca4 (gf_dump_vrml_field.isra+1332) ← mov edi, dword ptr [r12]

```

```

[
► 0x644ca4 <gf_dump_vrml_field.isra+1332> mov edi, dword ptr [r12]
  0x644ca8 <gf_dump_vrml_field.isra+1336> lea rbx, [rsp + 0x20]
  0x644cad <gf_dump_vrml_field.isra+1341> test edi, edi
  0x644caf <gf_dump_vrml_field.isra+1343> je gf_dump_vrml_field.isra+1344
    ↓
  0x644d08 <gf_dump_vrml_field.isra+1432> mov esi, dword ptr [r13 + 0x10]
  0x644d0c <gf_dump_vrml_field.isra+1436> mov rdi, qword ptr [r13 + 0x18]
  0x644d10 <gf_dump_vrml_field.isra+1440> test esi, esi
  0x644d12 <gf_dump_vrml_field.isra+1442> je gf_dump_vrml_field.isra+1443
    ↓
  0x644ea0 <gf_dump_vrml_field.isra+1840> xor eax, eax
  0x644ea2 <gf_dump_vrml_field.isra+1842> lea rsi, [rip + 0x5f4fd3]
  0x644ea9 <gf_dump_vrml_field.isra+1849> call gf_fprintf
]

```

```

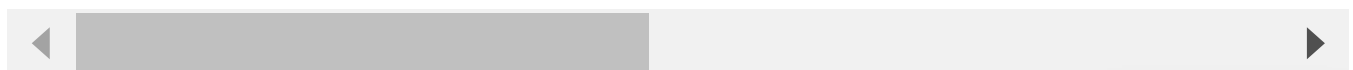
00:0000| rsp 0x7fffffff70c0 → 0xf392a0 ← 0x30646c6569665f /* '_field0' */,
01:0008|      0x7fffffff70c8 ← 0x40b8270500000038 /* '8' */
02:0010|      0x7fffffff70d0 → 0xf3b210 ← 0x0
03:0018|      0x7fffffff70d8 → 0xf3b210 ← 0x0
04:0020|      0x7fffffff70e0 → 0xf387d0 → 0xf37f10 ← 0x0
05:0028|      0x7fffffff70e8 → 0x7fffffff7114 ← 0xf38ab000000001
06:0030|      0x7fffffff70f0 ← 0x0
07:0038|      0x7fffffff70f8 ← 0x2

```

```

[ E
► f 0      0x644ca4 gf_dump_vrml_field.isra+1332
  f 1      0x6459ce gf_dump_vrml_node+1566
  f 2      0x642039 gf_sm_dump_command_list+873
  f 3      0x64908d gf_sm_dump+797
  f 4      0x41b5d8 dump_isom_scene+616
  f 5      0x4125ec mp4boxMain+9228
  f 6      0xb59600 __libc_start_main+1168

```



Chat with us

## CWE-476: NULL Pointer Dereference

### Severity

Medium (6.6)

### Visibility

Public

### Status

Fixed

### Found by



**zfeixq**

@zfeixq

unranked ▼

This report was seen 445 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

**zfeixq** 10 months ago

Researcher

Hello,

This bug seems to have been fixed on github, and the maintainer seems to have forgotten to click verify on huntr.

Thank you.

We have sent a follow up to the **gpac** team. We will try again in 7 days. 10 months ago

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

Maintainer

That's correct, see <https://github.com/gpac/gpac/issues/2055>.

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

Chat with us

A [gpac/gpac](#) maintainer marked this as fixed in [1.1.0](#) with commit [9f8510](#) 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us