NULL Pointer Dereference in gpac/gpac

Valid Reported on Dec 30th 2021

Description

Null Pointer Dereference in gf_utf8_wcslen ()

Proof of Concept

POC is here.

bt

```
Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------
RAX: 0x24 ('$')
RBX: 0x5555555e2870 --> 0x5555555e2840 --> 0x2000000020000000 ('')
RCX: 0x0
RDX: 0x7ffff697e740 (0x00007ffff697e740)
RSI: 0x0
RDI: 0x0
RBP: 0x2
RSP: 0x7fffffff7ff8 --> 0x7ffff78f7d71 (<xtra_box_dump+129>:    lea    ebx,
RIP: 0x7ffff77ac884 (<gf_utf8_wcslen+4>:    cmp    WORD PTR [rdi],0x0)
R8 : 0x0
R9 : 0x24 ('$')
R10: 0x7ffff7e0cbc7 --> 0x22 ('"')
R11: 0x7fffffff7ec7 --> 0x58c47a4e82a90030
R12: 0x5555555db220 --> 0x7ffffbad2c84
R13: 0x5555555e2920 --> 0x58747261 ('artX')
R14: 0x5555555e28a0 --> 0x0
R15: 0x7ffff7e71725 --> 0x2020200058323025 ('%02X')
EFLAGS: 0x10202 (carry parity adjust zero sign trap INTERRU
[-------------------------------------code-------------------------------------
```

```
   0x7ffff77ac874:  data16 nop WORD PTR cs:[rax+rax*1+0x0]
   0x7ffff77ac87f:  nop
   0x7ffff77ac880 <gf_utf8_wcslen>: endbr64

=> 0x7ffff77ac884 <gf_utf8_wcslen+4>:   cmp    WORD PTR [rdi],0x0
   0x7ffff77ac888 <gf_utf8_wcslen+8>:   je     0x7ffff77ac8a8 <gf_utf8_wcs]
   0x7ffff77ac88a <gf_utf8_wcslen+10>:  mov    rax,rdi
   0x7ffff77ac88d <gf_utf8_wcslen+13>:  nop    DWORD PTR [rax]
   0x7ffff77ac890 <gf_utf8_wcslen+16>:  add    rax,0x2
[----------------------------------stack-----------------------------------
0000| 0x7fffffff7ff8 --> 0x7ffff78f7d71 (<xtra_box_dump+129>:   lea    ebx,
0008| 0x7fffffff8000 --> 0x5555555db650 --> 0x73747473 ('stts')
0016| 0x7fffffff8008 --> 0x2
0024| 0x7fffffff8010 --> 0x0
0032| 0x7fffffff8018 --> 0x6458c47a4e82a900
0040| 0x7fffffff8020 --> 0x5555555db220 --> 0x7ffffbad2c84
0048| 0x7fffffff8028 --> 0x5555555da950 --> 0x0
0056| 0x7fffffff8030 --> 0x5555555e2920 --> 0x58747261 ('artX')
[----------------------------------------------------------------------------
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x00007ffff77ac884 in gf_utf8_wcslen () from /home/zxq/CVE_testing/source/g
gdb-peda$ bt
#0  0x00007ffff77ac884 in gf_utf8_wcslen () from /home/zxq/CVE_testing/sour
#1  0x00007ffff78f7d71 in xtra_box_dump () from /home/zxq/CVE_testing/sourc
#2  0x00007ffff78fa5f2 in gf_isom_box_dump () from /home/zxq/CVE_testing/sc
#3  0x00007ffff78e99f6 in gf_isom_dump () from /home/zxq/CVE_testing/source
#4  0x0000555555588c15 in dump_isom_xml ()
#5  0x000055555557c564 in mp4boxMain ()
#6  0x00007ffff74dc0b3 in __libc_start_main (main=0x55555556d420 <main>, ar
    at ../csu/libc-start.c:308
#7  0x000055555556d45e in _start ()
```

Impact

This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution.

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (5.5)

Visibility
Public

Status
Fixed

Found by

zfeixq
@zfeixq
unranked

This report was seen 544 times.

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

zfeixq a year ago Researcher

Command:
MP4Box -diso -out /dev/null POC

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

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

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

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-DEV HEAD** with com
10 months ago

The fix bounty has been dropped ×

This vulnerability will not receive a CVE ×

Sign in to join this conversation