huntr

Null Pointer Dereference Caused Segmentation Fault in gpac/gpac

✓ Valid) Reported on Jul 23rd 2022

Description

Null pointer dereference caused segmentation fault. This can cause Denial-of -service attack.

version

```
smlijun@ubuntu:~/gpac_asan/bin/gcc$ ./MP4Box -version
MP4Box - GPAC version 2.1-DEV-rev243-gf87b12b32-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io
Please cite our work in your research:
    GPAC Filters: https://doi.org/10.1145/3339825.3394929
    GPAC: https://doi.org/10.1145/1291233.1291452
GPAC Configuration:
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SOCK_UN GPAC_
```

Proof of Concept

PoC is available herePoC #Asan Log

```
smlijun@ubuntu:~/gpac asan/bin/gcc$ ./MP4Box -bt ../../gpac/bin/gcc/poc
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
                                                                Chat with us
[iso file] Unknown box type 0000 in parent moov
Fiso filel Unknown hox type 0000 in parent mooy
```

```
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent minf
[iso file] Missing DataInformationBox
[iso file] Unknown box type 0000 in parent moov
[iso file] Read Box type 0000 (0x30303030) at position 11542 has size 0 but
[iso file] Box "moov" (start 20) has 806 extra bytes
[iso file] Unknown top-level box type 0000
[iso file] Incomplete box 0000 - start 12356 size 808358436
[iso file] Incomplete file while reading for dump - aborting parsing
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent minf
[iso file] Missing DataInformationBox
[iso file] Unknown box type 0000 in parent moov
[iso file] Read Box type 0000 (0x30303030) at position 11542 has size 0 but
[iso file] Box "moov" (start 20) has 806 extra bytes
[iso file] Unknown top-level box type 0000
[iso file] Incomplete box 0000 - start 12356 size 808358436
[iso file] Incomplete file while reading for dump - aborting parsing
MPEG-4 BIFS Scene Parsing
[ODF] Reading bifs config: shift in sizes (not supported)
[MP4 Loading] Unable to fetch sample 38 from track ID 8 - aborting track in
Scene loaded - dumping 1 systems streams
AddressSanitizer: DEADLYSIGNAL
_____
==3541124==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000
==3541124==The signal is caused by a READ memory access.
==3541124==Hint: address points to the zero page.
    #0 0x7fa63fcdc017 in gf dump vrml simple field.isra.0 (/home/smlijun/gr
   #1 0x7fa63fcdcc1b in DumpXReplace (/home/smlijun/gpac asan/bin/gcc/libs
   #2 0x7fa63fcd728a in gf sm dump command list (/home/smlijun/gpac asan/k
   #3 0x7fa63fcde00c in gf sm dump (/home/smlijun/gpac asan/bin/gcc/libgpac
   #4 0x559fd823f0b7 in dump isom scene (/home/smlijun/gpac asan/bin/gcc/N
   #5 0x559fd8234b50 in mp4box_main (/home/smlijun/gpac_asər''
   #6 0x7fa63f77f082 in libc start main ../csu/libc-star
   #7 0x559fd822458d in start (/home/smlijun/gpac asan/bin/gcc/mr4box+vx1
```

[100 1110] OHRHOWH DON CYPE OOO IN PARCHE MOOV

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV (/home/smlijun/gpac_asan/bin/gcc/libgpac.sc ==3541124==ABORTING



Impact

This vuln is capable of DoS.

CVE

CVE-2022-2549 (Published)

Vulnerability Type

CWE-476: NULL Pointer Dereference

Severity

Medium (5.7)

Registry

Other

Affected Version

2.1-DEV-rev243-gf87b12b32-master

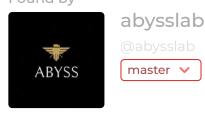
Visibility

Public

Status

Fixed

Found by



This report was seen 550 times.

Chat with us

A gpac/gpac maintainer 4 months ago

https://github.com/gpac/gpac/issues/2232

A gpac/gpac maintainer validated this vulnerability 4 months ago

abysslab 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 v2.1.0-DEV with commit 0102c5 4 months ago

The fix bounty has been dropped *

This vulnerability will not receive a CVE x

abysslab 4 months ago Researcher

@admin can we get a CVE for this?

Jamie Slome 4 months ago Admin

@maintainer - are you happy for a CVE to be assigned and published for this?

A gpac/gpac maintainer 4 months ago

Yes. You are asking us the same question for each report, would it be possible to store somewhere that we agree with submitting CVEs whenever appropriate?

Jamie Slome 4 months ago Admin

I've assigned a CVE for this report.

Regarding future reports, I will just proceed to assign and publish CVEs 👍

A gpac/gpac maintainer 4 months ago Thanks Sign in to join this conversation huntr part of 418sec