huntr

Segmentation Fault in SFS_Expression in gpac/gpac

0

✔ **Valid**   Reported on Jul 30th 2022

It can cause Denial-of-service attack.

Version

root@ubuntu:~/gpac/.git# cat refs/heads/master
0102c5d4db7fdbf08b5b591b2a6264de33867a07

system stack size (default)

root@ubuntu:~/gpac/bin/gcc# ulimit -s
8192

POC

Download POC

Execute

root@ubuntu:~/gpac/bin/gcc# ./MP4Box -info -disox -dump-chap-ogg -dump-cove
[iso file] Unknown box type FF0000 in parent moov
[iso file] extra box maxr found in hinf, deleting
[iso file] Unknown box type 80000 in parent moov
[iso file] Incomplete box mdat - start 11495 size 808395597
[iso file] Incomplete file while reading for dump - aborting parsing
[iso file] Unknown box type FF0000 in parent moov
[iso file] extra box maxr found in hinf, deleting
[iso file] Unknown box type 80000 in parent moov
[iso file] Incomplete box mdat - start 11495 size 808395597
[iso file] Incomplete file while reading for dump - aborting parsing

Chat with us

GDB

```
#1 ...
#7880 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7881 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7882 0x00007ffff6cdc89f in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7883 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7884 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7885 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7886 0x00007ffff6cdc89f in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7887 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7888 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7889 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7890 0x00007ffff6cdc89f in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7891 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7892 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7893 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7894 0x00007ffff6cdc89f in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7895 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7896 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7897 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7898 0x00007ffff6cdc89f in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7899 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7900 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7901 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7902 0x00007ffff6cdc89f in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7903 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7904 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7905 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7906 0x00007ffff6cdc89f in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7907 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7908 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7909 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
#7910 0x00007ffff6cdc89f in SFS_Expression (parser=0x7fffff
#7911 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7fffff
#7912 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7ffffff6f30) at bifs/
```

Chat with us

```
#7913 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7fffffff6f30) at bifs/
#7914 0x00007ffff6cdc89f in SFS_Expression (parser=0x7fffffff6f30) at bifs/
#7915 0x00007ffff6cdcc25 in SFS_Expression (parser=0x7fffffff6f30) at bifs/
#7916 0x00007ffff6cdbf19 in SFS_Expression (parser=0x7fffffff6f30) at bifs/
#7917 0x00007ffff6cdc6c7 in SFS_Expression (parser=0x7fffffff6f30) at bifs/
#7918 0x00007ffff6cdb61c in SFS_CompoundExpression (parser=0x7fffffff6f30)
#7919 0x00007ffff6cdaed3 in SFS_IfStatement (parser=0x7fffffff6f30) at bifs
#7920 0x00007ffff6cdac78 in SFS_Statement (parser=0x7fffffff6f30) at bifs/s
#7921 0x00007ffff6cdab2c in SFS_StatementBlock (parser=0x7fffffff6f30, func
#7922 0x00007ffff6cd9f01 in SFScript_Parse (codec=<optimized out>, script_
#7923 0x00007ffff6cc5563 in gf_bifs_dec_sf_field (codec=0x8de970, bs=0x8cde
#7924 0x00007ffff6cc9156 in BD_DecMFFieldVec (codec=0x8de970, bs=0x8cded0,
#7925 0x00007ffff6cc9a74 in gf_bifs_dec_field (codec=0x8de970, bs=0x8cded0,
#7926 0x00007ffff6cca419 in gf_bifs_dec_node_list (codec=0x8de970, bs=0x8cc
#7927 0x00007ffff6cc8130 in gf_bifs_dec_node (codec=0x51, bs=<optimized out
#7928 0x00007ffff6cc8daa in BD_DecMFFieldVec (codec=0x8de970, bs=0x8cded0,
#7929 0x00007ffff6cc9a74 in gf_bifs_dec_field (codec=0x8de970, bs=0x8cded0,
#7930 0x00007ffff6cca419 in gf_bifs_dec_node_list (codec=0x8de970, bs=0x8cc
#7931 0x00007ffff6cc8130 in gf_bifs_dec_node (codec=0x37, bs=<optimized out
#7932 0x00007ffff6cb5067 in BD_DecSceneReplace (codec=0x8de970, bs=0x8cded0
#7933 0x00007ffff6cd6043 in BM_SceneReplace (codec=0x8de970, bs=0x6, com_li
#7934 0x00007ffff6cd6556 in BM_ParseCommand (codec=0x8de970, bs=0x8cded0, c
#7935 0x00007ffff6cd7075 in gf_bifs_decode_command_list (codec=0x8de970, ES
      data=0x8dedb0 "\314\314", '\060' <repeats 169 times>, "\020", '\060' <r
#7936 0x00007ffff70b378e in gf_sm_load_run_isom (load=0x7fffffff8660) at sc
#7937 0x00007ffff70765ab in gf_sm_load_run (load=0x7fffffff8660) at scene_m
#7938 0x0000000000443136 in dump_isom_scene (file=<optimized out>, inName=0
      do_log=<optimized out>, no_odf_conv=<optimized out>) at filedump.c:203
#7939 0x0000000000434038 in mp4box_main (argc=<optimized out>, argv=<optimi
#7940 0x00007ffff657ec87 in __libc_start_main (main=0x4410a0 <main>, argc=0
      stack_end=0x7fffffffe478) at ../csu/libc-start.c:310
#7941 0x00000000004103fa in _start
```

◀   ▶
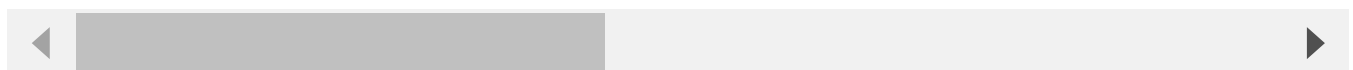
Impact

DoS

Chat with us

CVE

CVE-2022-3222
(Published)

Vulnerability Type

CWE-674: Uncontrolled Recursion

Severity

Medium (5.3)

Registry
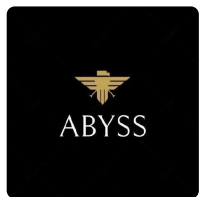
Other

Affected Version

stable

Visibility

Public

Status

Fixed

Found by

abysslab

@abysslab

master ⌄

We are processing your report and will contact the **gpac** team within 24 hours.   4 months ago

We have contacted a member of the **gpac** team and are waiting to hear back   4 months ago

A **gpac/gpac** maintainer   4 months ago   Maintainer

https://github.com/gpac/gpac/issues/2238

We have sent a follow up to the **gpac** team. We will try again in 7 days.   4 months ago

We have sent a second follow up to the **gpac** team. We will try again in 10 days.   4 months ago

We have sent a third and final follow up to the **gpac** team. This report is no
3 months ago

Chat with us

A **gpac/gpac** maintainer validated this vulnerability 2 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 **2.1.0-DEV** with commit **4e7736** 2 months ago

The fix bounty has been dropped   ✖

This vulnerability will not receive a CVE   ✖

abysslab 2 months ago   Researcher

Can we get CVE ID?

abysslab 2 months ago   Researcher

@admin

Jamie Slome 2 months ago   Admin

Sorted 👍

Sign in to join this conversation

Chat with us

huntr   part of 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us