

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
55658 -
Floating-
point
Exception
in
GPAC/MP4
Box

Processing
a crafted
MP4 file
containing
malformed
Opus audio
metadata
with
`MP4Box`
can trigger
a floating-
point
exception
in
`gf_opus_p
arse_packe
t_header()`
causing a
process
crash.

Summary:
The

Create account

Login



arse_packet_header() function in media_tools/av_parsers.c does not sufficiently validate critical Opus packet header fields before using them in arithmetic operations. In the observed crash, malformed Opus packet data reaches the parser with invalid frame/header parameters. The code then performs arithmetic on these values, including a

[Create account](#)[Login](#)

involving
`header-
>nb_frame
s`, and
triggers a
floating-
point
exception.

AddressSa
nitizer
reports an
`FPE` at
`media_too
ls/av_parse
rs.c:11479`
while
MP4Box
exports or
inspects
the crafted
MP4
through the
Opus dump
path.

CWE:
CWE-369 -
Divide by
Zero

Affected
Component:
...

media_tool
s/av_parse
rs.c:11479
Function:

[Create account](#)[Login](#)

```
rse_packet  
_header()
```

```
filters/insp  
ect.c:1830  
Function:  
gf_inspect_  
dump_opu  
s_internal()
```

```
application  
s/mp4box/  
filedump.c:  
1501  
Function:  
dump_iso  
m_opus()  
...
```

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
MP4Box
versions
2.4 and
earlier
(GPAC
build at
commit:
ff8249a40
7685d00ce
156110750)

[Create account](#)[Login](#)

8b9cad195
140e)

Attack
Conditions:
An attacker
supplies a
crafted
MP4 file
containing
an Opus
audio track
with
malformed
packet/hea
der
parameters
. The issue
can be
reproduced
locally
with:

```
...  
./MP4Box -  
add  
2_poc.mp4  
-dxml -out  
/dev/null  
...
```

No
elevated
privileges
are
required.
User
interaction
is required

[Create account](#)[Login](#)

manually
processes
the
malicious
MP4 file, or
an
automated
workflow
invokes
MP4Box on
attacker-
controlled
media.

Impact:
The
immediate
observed
impact is
Denial of
Service due
to an
uncaught
floating-
point
exception
and
process
termination
. No
evidence of
arbitrary
code
execution
was
observed
for this
crash.

[Create account](#)[Login](#)

status:

The issue
was fixed
in GPAC
commit:

...

ed66d9c85
731902576
5e0587f2e
a291e1456
58da

...

Users
should
update to a
GPAC build
containing
this
commit or
later. The
parser
should
reject
malformed
Opus
packet
headers
before
performing
arithmetic
on fields
such as
frame
count, TOC-
derived
values, or
packet

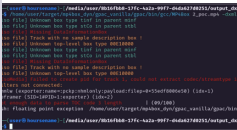
[Create account](#)[Login](#)

derived values.

References:

- Issue: [github.com/gpac/gpac/issues/31...](#)
- PoC: [github.com/sigdevel/pocs/blob/...](#)
- Fix: [github.com/gpac/gpac/commit/ed...](#)

Credit @sigdevel



- #fuzzing
- #infosec
- #security

...and 10 more

Jun 07, 2026, 06:25 PM

Last edited Jun 07, 07:24 PM

—

|

|

Create account

Login