

[← P...](#) 

sigd...
@si...

Security
Advisory:
CVE-2025-
55642 -
Divide by
Zero in
GPAC
MP4Box
AVI
Demuxer

Processing
a crafted
AVI-like
media file
with
`MP4Box`
can trigger
a division
by zero in
`avidmx_pr
ocess()`,
causing a
floating-
point
exception
and Denial
of Service.

Summary:
The
`avidmx_pr
ocess()`
function in

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

x_avi.c` does not sufficiently validate frame-count metadata before using it as a divisor during bitrate computation. When MP4Box processes a specially crafted input with invalid AVI frame metadata, such as a `0/256` frame declaration, the DASH processing path attempts to compute bitrate from the bitstream and divides by zero. AddressSanitizer reports an

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

`filters/dm
x_avi.c:639
`
`.

CWE:
CWE-369 -
Divide by
Zero

Affected
Componen
t:
`

filters/dmx
_avi.c:639
Function:
avidmx_pro
cess()
`

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
GPAC
MP4Box
v2.4 is
affected
according
to the CVE
request
data. The

Create account

Login

on a GPAC
build at
commit:
...

f87b30611
380e4dcd0
3cd4dd9ac
553c0ec33
6826
...

Builds
before the
fix commit
`cea49f684
dbc4d53ec
d6c76a962
3838802a6
8d88`
should be
considered
affected if
they
contain the
vulnerable
AVI
demuxer
bitrate
computatio
n path.

Attack
Conditions:
An attacker
supplies a
crafted
AVI-like
media file
with invalid

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

The issue is triggered while processing the file through MP4Box DASH segmentation, for example with a `dash` command using `14\_poc.mp4`. No elevated privileges are required. User interaction is required when the victim manually processes the malicious media file, or an automated workflow invokes MP4Box on attacker-controlled

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

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.

Fix / mitigation status:

The issue was fixed in GPAC commit: ...

cea49f684
dbc4d53ec
d6c76a962
3838802a6
8d88
...

Users should

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

containing this commit or later. The affected code should validate ``num_frames`` and related AVI metadata before using frame counts in bitrate calculations.

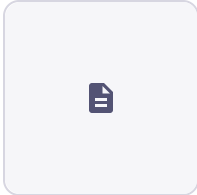
References

- Issue: github.com/gpac/gpac/issues/311
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/ce...

Credit:
[@sigdevel](#)

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

A.
Shvedov)



- #fuzzing
- #infosec
- #security

...and 11 more

Jun
12,
2026, · 🌐 · We
11:00
AM

Last edited
Jun 12, 11:23
AM

0 boosts · 0 qu



EN 🗨️ 🌐

 @sig
devel
Hello
,
pleas
e
add
direc
t
refer
ence
s to
the
CVE
too.

there is only this Mastodon toot. Please add directly reference also to the "Issue", "PoC" and "Fix" you have shared in this too.

Thanks!

🔙 0