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_process()`, causing a floating-point exception and Denial of Service.

Summary: The `avidmx_process()` 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/dmx_avi.c:639`.

CWE: CWE-369 - Divide by Zero

Affected Component:
```
filters/dmx_avi.c:639
Function: avidmx_process()
```

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:
```
f87b30611380e4dcd03cd4dd9ac553c0ec336826
```

Builds before the fix commit `cea49f684dbc4d53ecd6c76a9623838802a68d88` should be considered affected if they contain the vulnerable AVI demuxer bitrate computation 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:
```
cea49f684dbc4d53ecd6c76a9623838802a68d88
```
Users should

Create account Login

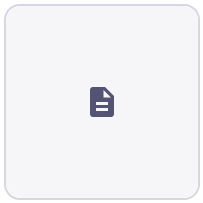
containing this commit or later. The affected code should validate `num_frames` and related AVI metadata before using frame counts in bitrate calculations.

References:
- Issue: github.com/gpac/gpac/issues/31…
- 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, 11:00 AM · · We

Last edited **Jun 12, 11:23 AM**

boosts · qu

Create account Login

Create account Login