Skip to main content 1
Skip to main navigation 2

Pos

sigd...
@si...

Security Advisory: CVE-2025-55651 - NULL Pointer Dereference in GPAC MP4Box

Processing a crafted or truncated MP4 file with `MP4Box` can trigger a NULL pointer dereference in `gf_isom_get_user_data_count()`, causing a Denial of Service.

Summary: The `gf_isom_get_user_dat

`isomedia/isom_read.c` does not verify that the UUID pointer passed to it is non-NULL before using it in a comparison. When MP4Box processes a malformed or truncated MP4 file, the isomedia input setup path can pass a NULL UUID pointer into `gf_isom_get_user_data_count()`.

AddressSanitizer reports a `SEGV` caused by a `READ` memory access at

000000`, with the crash occurring at `isomedia/isom_read.c:2754`.

CWE: CWE-476 - NULL Pointer Dereference

Affected Component:
```
isomedia/isom_read.c:2754
Function: gf_isom_get_user_data_count()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected

versions 2.4 and earlier (GPAC build at commit: 46be5f928660530d5332cd2f1d1772087375 58ef)

Attack Conditions: An attacker supplies a crafted or truncated MP4 file. The issue can be reproduced locally with a command of this form:

```
./MP4Box -add 4_poc.mp4 -new /dev/null -split-size 5000000
```

No

are required. User interaction is required when the victim 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 process termination. The crash is a NULL pointer dereference on the zero page; no evidence of arbitrary

was observed.

Fix / mitigation status: The issue was fixed in GPAC commit:

```
921d2a133779c9b01cb4016cecdd929609745ad0
```

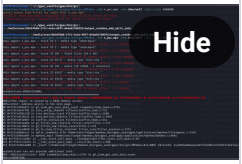
Users should update to a GPAC build containing this commit or later. The affected code should validate UUID pointers and reject malformed /truncated MP4 structures before

n routines on user-data UUID values.

References:

- Issue: github.com/gpac/gpac/issues/31...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/92...

Credit @sigdevel



#fuzzing

#infosec

#security

...and 10 more

Jun 07, 2026, 07:38 PM · · We

Last edited
Jun 07, 07:39 PM

0 boosts · **0** qu

Create account Login