Skip to main content 1
Skip to main navigation 2

Pos

sigd...
@si...

Security Advisory: CVE-2025-60485 - NULL Pointer Dereference in GPAC/MP4 Box

Processing a crafted MP4 file with corrupted `esds` boxes and incomplete box structures triggers a NULL pointer dereference in `gf_isom_apple_set_tag_ex`, causing MP4Box to crash.

Summary: The `gf_isom_apple_set_tag_ex` function in `isomedia/isom_write.c` is called during muxer tag setup to write Apple metadata tags into the output file. When the input MP4 contains an invalid `esds` descriptor (tag 3, truncated size) and an incomplete box structure, the function receives an unvalidated NULL pointer and dereferences it (READ at address

without a prior NULL check, terminating the process with SIGSEGV.

CWE: CWE-476 - NULL Pointer Dereference

Affected Component:
```
isomedia/isom_write.c:6309
Function: gf_isom_apple_set_tag_ex()

filters/mux_isom.c:841
Function: mp4_mux_set_tags()
```

Affected Product: MP4Box

Open Source Project)

Affected Version: 2.5-DEV-rev1687-ge44a4e2b0-master; commit `e44a4e2b0d193566619ada71599e70255699da94`. Any codebase equivalent to this commit that has not applied the fix commit is affected.

Attack Conditions: An attacker supplies a crafted MP4 file containing a corrupted `esds` box (invalid descriptor sizes) and

structures. Local access is required; the victim must invoke `MP4Box -add <crafted_file>` or any equivalent MP4Box operation that triggers the muxer PID setup and tag-writing path.

Impact: The NULL pointer dereference (READ at address 0x000000000000) causes an immediate process crash, resulting in Denial of Service. No evidence of arbitrary code

observed; the faulting access is a NULL read that is not exploitable for control-flow hijacking.

Fix / mitigation status: The fix adds a NULL check for the tag pointer before dereferencing it in `gf_isom_apple_set_tag_ex`. Users should upgrade to the release containing commit `4860a1a6f128ccc9ae37b4b738d22029f9672457` or apply that patch directly.

- Issue: github.com/gpac/gpac/issues/33...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/48...

Credit @sigdevel

#fuzzing
#infosec
#security
...and 9 more

May 30, 2026, · · We 08:07 AM

Last edited **May 30, 08:20 AM**

0 boosts · **0** qu