sigd...
@si...

Security Advisory: CVE-2025-60495 - NULL Pointer Dereference in GPAC/MP4Box

Processing a crafted MP4 file with an inconsistent video sample entry triggers a NULL pointer dereference in `gf_media_get_color_info`, causing MP4Box to crash.

Summary: The `gf_media

nfo` function in `media_tools/isom_tools.c` inspects codec-specific boxes nested inside a video sample entry. When a sample entry type (e.g., `v210`) unexpectedly contains an unrelated box (e.g., an `avcC` AVC Decoder Configuration Box), the function dereferences a near-NULL pointer (READ at address 0x0000000

NULL-check is performed before the dereference, and the process terminates with SIGSEGV.

CWE: CWE-476 - NULL Pointer Dereference

Affected Component

```
media_tools/isom_tools.c:979
Function: gf_media_get_color_info()
```

Affected Product: MP4Box (GPAC Multimedia Open Source

Affected Version: 2.5-DEV-rev1780-g50b5741f2-master; commit `50b5741f291126b610c59db433fc02e8a17f0c5d`. Any codebase equivalent to this commit that has not applied the fix commit is affected.

Attack Conditions: An attacker supplies a specially crafted MP4 file containing a video sample entry whose type (e.g., `v210`) holds an incompatib le child box

Local access is required; the victim must process the file with `MP4Box -split-size 8000 <crafted_file>` or any equivalent MP4Box operation that triggers muxer PID setup.

Impact: The NULL pointer dereference (READ at address 0x8) causes an immediate process crash, resulting in Denial of Service. No evidence of arbitrary code execution was

access is a near-NULL read that is not exploitable for control-flow hijacking.

Fix / mitigation status: The fix adds the missing NULL check in `gf_media_get_color_info` before dereferencing the color-info pointer. Users should upgrade to the release containing commit `9beed3c0a2f38505c745e5376234e7ed66e8e0b1` or apply that patch directly.

- PoC: github.com/sigdevel/pocs/blob/...
- Issue: github.com/gpac/gpac/issues/33...
- Fix: github.com/gpac/gpac/commit/9b...

Credit @sigdevel

#fuzzing

#infosec

#security

...and 9 more

May 29, 2026, · · We 05:32 PM

0 boosts · **0** qu