sigd...
@si...

Security Advisory: CVE-2025-60483 - NULL Pointer Dereference in GPAC/MP4 Box

Processing a crafted AC-4 stream triggers a NULL pointer dereference in `gf_ac4_pres_b_4_back_channels_present` when accessing presentation data with an invalid substream group index, causing

Summary: The `gf_ac4_pres_b_4_back_channels_present` function in `media_tools/av_parsers.c` accesses `pres->substream_groups` using an index derived from the stream. When a crafted AC-4 file specifies an invalid group index (e.g., group 4 that does not exist for presentation 0), the parser dereferences a NULL or near-NULL pointer at address

byte struct offset) without first validating the pointer or the group index bounds. The process terminates with SIGSEGV.

CWE: CWE-476 - NULL Pointer Dereference

Affected Component

```
media_tools/av_parsers.c:15703
Function: gf_ac4_pres_b_4_back_channels_present()
```

Affected

(GPAC Multimedia Open Source Project)

Affected Version: 2.5-DEV-rev1617-g856674b22-master; commit `856674b226d6cbe28a941ad223be38194cbf7d37`. Any codebase equivalent to this commit that has not applied the fix commit is affected.

Attack Conditions: An attacker supplies a specially crafted AC-4 stream file containing an invalid substream

Local access is required; the victim must invoke `MP4Box -dash 100 <crafted_file>` or any equivalent DASH segmentation command that triggers the AC-4 demuxer and presentation parsing path.

Impact: The near-NULL pointer dereference (READ at address 0x000000000048) causes an immediate process crash, resulting in Denial of

arbitrary code execution was observed; the faulting access is a near-NULL read that is not exploitable for control-flow hijacking.

Fix / mitigation status: The fix adds bounds validation for the substream group index and a NULL check for the presentation pointer in `gf_ac4_pres_b_4_back_channels_present`. Users should upgrade to the release

`13eb5b76560aaf7813b865a2ad433258478e2695` or apply that patch directly.

References

- Issue: github.com/gpac/gpac/issues/33...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/13...

Credit @sigdevel

#fuzzing

#infosec

#security

...and 9 more

May 29, 2026 · · We