P...



sigd...
@si...

Security Advisory: CVE-2025-60488 - NULL Pointer Dereference in GPAC/MP4Box

Processing a crafted MP4 file with a missing Sample Description box triggers a NULL pointer dereference in `dump_isom_saps`, causing MP4Box to crash.

Summary: The `dump_isom_saps`

Create account Login

`applications/mp4box/filedump.c` iterates over track metadata to dump SAP (Sync Access Point) information. When the input MP4 contains a corrupted track structure where the Sample Description box (`stsd`) is absent, the function accesses track metadata pointers without prior validation, dereferencing a near-NULL address (0x1c, 28-byte struct offset) and

Create account Login

triggering SIGSEGV.

CWE: CWE-476 - NULL Pointer Dereference

Affected Component:
```
applications/mp4box/filedump.c:1743
Function: dump_isom_saps()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version: 2.5-DEV-rev1672-gc9a31d0e1-master; commit

Create account Login

14c6d81c5461859ed63d075`. Any codebase equivalent to this commit that has not applied the fix commit is affected.

Attack Conditions: An attacker supplies a crafted MP4 file whose track structure lacks a valid `stsd` box. Local access is required; the victim must invoke `MP4Box -dsap 1 <crafted_file>` or any equivalent SAP analysis command

Create account Login

the SAP dump path.

Impact: The near-NULL pointer dereference (READ at address 0x0000000 0001c) causes an immediate process crash, resulting in Denial of Service. No evidence 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 issue

Create account Login

commit:
```
e6d01820d7bf3967d931fedb379ee5f209bc133b
```
Users should update to a GPAC build containing this commit or later.

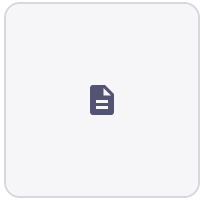
References:

- Issue: github.com/gpac/gpac/issues/33...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/e6...

Credit Alexander A. Shvedov (@sigdevel

Create account Login

#fuzzing #infosec #security #afl++ #revers #cybersecurity #bugbounty #vulnerability #opensource #linux #cve #advisory #gpac



Oct 17, 2026, · · We 02:10 PM

0 boosts · **0** qu

Create account Login