Skip to main content 1
Skip to main navigation 2

P...

sigd...
@si...

Security Advisory: CVE-2025-55639 - NULL Pointer Dereference in GPAC MP4Box Track Kind Handling

Processing a crafted MP4 file with MP4Box `-add` can trigger a NULL pointer dereference in `gf_isom_add_track_kind()`, causing a Denial of Service.

Summary: The

nd()` function in `isomedia/isom_write.c` does not sufficiently validate the `kind` string before passing it to `strdup()`. When MP4Box imports a specially crafted MP4 file containing corrupted MPEG-2 TS PMT descriptors and empty track metadata, a NULL `kind` pointer can reach `gf_isom_add_track_kind()`.

AddressSanitizer reports a segmentati

a read from address `0x0` in `strlen()` during `strdup()`, reached from `gf_isom_add_track_kind()` at `isomedia/isom_write.c:3153`.

CWE: CWE-476 - NULL Pointer Dereference

Affected Component:
```
isomedia/isom_write.c:3153
Function: gf_isom_add_track_kind()
```

Affected Product: MP4Box (GPAC

Source Project)

Affected Version: MP4Box version 2.4 is affected according to the prepared CVE/MITRE data. The issue was reproduced on a GPAC build at commit:
```
78c2c9be29a41b38eca2c53d280442088a71dab9
```
Builds before the fix commit `027ce139dda498ee95df36db9f9f6f3cadce8ec9` should be considered affected if they contain the vulnerable

handling path.

Attack Conditions: An attacker supplies a crafted MP4 file with corrupted PMT descriptors in an MPEG-2 TS stream and malformed or empty track metadata. The issue can be reproduced locally with:

```
./MP4Box -add 23_poc.mp4 -new /dev/null
```

No elevated privileges are required.

is required when the victim manually processes the malicious file, or an automated media workflow invokes MP4Box on attacker-controlled input.

Impact: The immediate observed impact is Denial of Service due to process termination. No evidence of arbitrary code execution was observed.

Fix / mitigation status: The issue was fixed

```
027ce139dda498ee95df36db9f9f6f3cadce8ec9
```

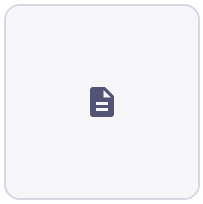
Users should update to a GPAC build containing this commit or later. The affected track metadata path should validate `kind` before duplicating it and fail cleanly when malformed input omits the expected metadata.

References:

- Issue: github.com

2...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/02...
- CVE record: cve.org/CVERecord?id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)



#fuzzing
#infosec
#security
...and 11 more

Jun 18, 2026, 04:19 AM · · We

0 boosts · 0 qu