Skip to main content 1
Skip to main navigation 2

Pos

sigd...
@si...

Security Advisory: CVE-2025-55659 - NULL Pointer Dereference in GPAC MP4Box `ctts_box_write`

Processing a crafted or truncated MP4 file with `MP4Box` can trigger a NULL pointer dereference in `ctts_box_write()`, causing a Denial of Service.

Summary: The `ctts_box_

`isomedia/box_code_base.c` does not sufficiently validate critical pointers and timestamp-derived state when writing the composition time-to-sample (`ctts`) box. When MP4Box processes a crafted truncated MP4 file during split/remux operations, negative timestamp handling can leave the composition-time entries pointer in an invalid or NULL state. The write path

dereferences the NULL pointer and crashes.

AddressSanitizer reports a `SEGV` caused by a `READ` memory access at address `0x000000000000`, with the crash occurring at `isomedia/box_code_base.c:464`.

CWE:
CWE-476 - NULL Pointer Dereference

Affected Component:
```
isomedia/box_code_b
```

ctts_box_write()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version: MP4Box versions 2.4 and earlier are affected according to the prepared CVE/MITRE data. The issue was reproduced on a GPAC build at commit:

```
ff8249a407685d00ceb5f4d2a798b9cad195140e
```
```

fix commit `2476b14058761845ad6ccee43dcf5d49ca9cca95` should be considered affected if they contain the vulnerable `ctts_box_write()` path.

Attack Conditions: An attacker supplies a crafted or truncated MP4 file with timestamp data that causes invalid negative timestamp handling during split/remux processing. The issue can be reproduced locally with:

```
./MP4Box -add 5_poc.mp4 -new ./test -split-size 500
```

No elevated privileges are required. User interaction is required when the victim manually processes the malicious MP4 file, or an automated workflow invokes MP4Box on attacker-controlled media.

Impact: The immediate observed impact is Denial of

termination. The crash is a NULL pointer dereference on the zero page; no evidence of arbitrary code execution was observed.

Fix / mitigation status: The issue was fixed in GPAC commit:

```
2476b14058761845ad6ccee43dcf5d49ca9cca95
```

Users should update to a GPAC build containing this commit or later. The

should validate compositio n-time entries and timestamp-derived state before writing the `ctts` box, and malformed /truncated MP4 inputs should be rejected cleanly.

References :

- Issue: github.com /gpac/gpa c/issues/3 1…
- PoC: github.com /sigdevel/p ocs/blob/…
- Fix: github.com /gpac/gpa c/commit/ 24…

Credit @sigdevel

GitHub

isome… NULL…

By **sigdevel**

#fuzzing

#infosec

#security

…and 10 more

Jun 07, 2026, · · We 08:36 PM

1 boost · **0** quo

Create account Login