Skip to main content 1
Skip to main navigation 2

Pos

sigd...
@si...

Security Advisory: CVE-2025-55641 - NULL Pointer Dereference in GPAC MP4Box Sample Info Copy

Processing a crafted MP4 file with corrupted Sample Auxiliary Information metadata can trigger a NULL pointer dereference in `gf_isom_copy_sample_info()`, causing a Denial of Service and

corruption impact.

Summary: The `gf_isom_copy_sample_info()` function in `isomedia/isom_write.c` does not sufficiently validate pointers after handling invalid Sample Auxiliary Information (SAI) metadata. A crafted MP4 file can provide corrupted SAI values, such as an invalid `sai_samples` count, causing memory allocation or merge handling to fail. The import

copy sample information from a NULL pointer.

AddressSanitizer reports a `SEGV` caused by a `READ` memory access at address `0x000000000000`, with the crash occurring at `isomedia/isom_write.c:8164`.

CWE: CWE-476 - NULL Pointer Dereference

Affected Component:
```
isomedia/isom_write.
```

gf_isom_copy_sample_info()
```

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:
```
f87b30611380e4dcd03cd4dd9ac553c0ec336826
```
```

An attacker supplies a crafted MP4 file containing corrupted SAI metadata. The issue can be reproduced locally with:

```
./MP4Box -add 13_poc.mp4 -new /dev/null -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 input.

Impact: The immediate observed impact is Denial of Service due to process termination. The local CVE/MITRE data also marks potential code execution impact; the observed ASAN trace is a NULL pointer read.

Fix / mitigation status: The issue was fixed in GPAC commit:
```
e38d24b7e
```

90ac3f2080b52
```

Users should update to a GPAC build containing this commit or later. The affected code should validate SAI metadata, allocation results, and sample-info pointers before copying sample information.

References:
- Issue: github.com/gpac/gpac/issues/31...
- PoC: github.com/sigdevel/pocs/blob/...
```

/gpac/gpac/commit/e3...

Credit: @sigdevel (Alexander A. Shvedov)

GitHub

[securi... isome...

By **sigdevel**

#fuzzing

#infosec

#security

...and 11 more

Jun 12, 2026, 10:57 AM · We

Last edited **Jun 12, 11:23 AM**

1 boost · **0** quo

Create account Login