

sigd...
@si...

Security Advisory: CVE-2025-55640 - Heap Buffer Overflow in GPAC MP4Box Sample Size Handling

Processing a crafted MP4 file with MP4Box `-add` can trigger a heap buffer overflow in `stbl_AddSize()`, causing a crash and potential code execution.

Summary: The `stbl_AddSize()`

Create account Login

	`isomedia/stbl_write.c` does not sufficiently validate sample count boundaries before writing to the sample size table. When MP4Box imports a specially crafted MP4 file containing manipulated sample metadata, corrupted sample counts, invalid aspect ratios, and oversized box declarations, the vulnerable path writes beyond the allocated heap buffer for `stbl->sampleSiz	

Create account Login

AddressSanitizer reports a `heap-buffer-overflow` at `isomedia/stbl_write.c:492`, with a `WRITE of size 4` immediately after a 64-byte heap allocation.

CWE: CWE-122 - Heap-based Buffer Overflow

Affected Component:
```
isomedia/stbl_write.c:492
Function: stbl_AddSize()
```

Affected Product:

Create account Login

Multimedia Open Source Project)

Affected Version: GPAC MP4Box version 2.4 is affected according to the prepared CVE/MITRE data. The issue was reproduced on a GPAC build at commit:
```
027ce139dda498ee95df36db9f9f6f3cadce8ec9
```
Builds before the fix commit `321624f28d19a413449fd1718d1eb59037f8f7fc` should be considered affected if

Create account Login

vulnerable sample size table update path.

Attack Conditions: An attacker supplies a crafted MP4 file with manipulated sample metadata. The issue can be reproduced locally with:

```
./MP4Box -add 25_poc.mp4 -new /dev/null
```

No elevated privileges are required. User interaction is required when the

Create account Login

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. Because the vulnerability is an out-of-bounds heap write, memory corruption and potential arbitrary code execution are possible.

Fix /

Create account Login

The issue was fixed in GPAC commit:
```
321624f28d19a413449fd1718d1eb59037f8f7fc
```
Users should update to a GPAC build containing this commit or later. The affected sample size table path should validate `sampleCount` and ensure capacity before writing sample size entries.

References:

- Issue:

Create account Login

c/issues/32...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/32...
- CVE record: cve.org/CVERecord?id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)



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

Jun 18, 2026, · · We 04:41 AM

0 boosts · 0 qu

Create account Login



Create account Login