Skip to main content 1
Skip to main navigation 2

Pos

sigd...
@si...

Security Advisory: CVE-2025-55647 - Integer Overflow in GPAC MP4Box PSSH Handling

Processing a crafted MP4 file with malformed Protection System Specific Header (PSSH) data can trigger an integer overflow and uncontrolled allocation in `mp4_mux_cenc_insert

Denial of Service through memory exhaustion.

Summary: The `mp4_mux_cenc_insert_pssh()` function in `filters/mux_isom.c` does not sufficiently validate PSSH sizes before allocating memory. A crafted MP4 file can set PSSH-related fields such as `kid_count` or `dataSize` to very large values. This can overflow the buffer size calculation

attempt a very large allocation during DASH/mux processing.

AddressSanitizer reports an out-of-memory condition at `filters/mux_isom.c:4326`, where `realloc()` attempts to allocate `0xe4000100` bytes.

CWE: CWE-190 - Integer Overflow or Wraparound

Affected Component:
```
filters/mux_isom.c:4326
Function:
```

_pssh()
```

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:
```
e95f3064d846e4606276fff111e0f97df1576a04
```
Builds before the fix commit
```

7ba06618bff9d587141792` should be considered affected if they contain the vulnerable PSSH allocation path.

Attack Conditions: An attacker supplies a crafted MP4 file containing malformed PSSH/CENC metadata. The issue can be reproduced locally with:
```
./MP4Box -dash 10000 ./15_poc.mp4
```
No elevated privileges

User interaction is required when the victim manually processes the malicious MP4 file, or an automated media workflow invokes MP4Box on attacker-controlled input.

Impact: The immediate observed impact is Denial of Service due to memory exhaustion and process termination. Because the root cause is an integer overflow in allocation-size

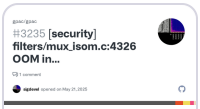
corruption and potential arbitrary code execution cannot be ruled out.

Fix / mitigation status:
The issue was fixed in GPAC commit:
```
2a1f638534cddf511a7ba06618bff9d587141792
```

References:
- Issue: github.com/gpac/gpac/issues/32...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/

fix/reference: github.com/gpac/gpac/commit/31...

Credit: @sigdevel (Alexander A. Shvedov)



GitHub

[securi... filters/...

By **sigdevel**

#fuzzing

#infosec

#security

...and 11 more

Jun 12, 2026, 11:02 AM · · We

2 boosts · **0** qu