sigd...
@si...

Security Advisory: CVE-2025-60486 - Use-After-Free in GPAC/MP4Box

Processing a crafted MPEG-2 Transport Stream file with corrupted PMT descriptors triggers a heap use-after-free in `dasher_process`, causing MP4Box to crash and potentially enabling arbitrary code execution.

Summary:
The

nfigure_pid ` function in `filters/das her.c` frees a PID context structure at line 976 when reconfiguri ng a stream. The freed pointer is not cleared, and `dasher_pr ocess` subsequen tly accesses the same memory at line 9445 during the next processing cycle. A crafted MPEG-2 TS file with repeated sync marker violations, broken PMT descriptors

conflicting PIDs triggers this reconfiguration sequence, leading to a READ of 4 bytes into freed heap memory.

CWE: CWE-416 - Use After Free

Affected Component:
```
filters/dasher.c:9445
Function: dasher_process()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected

rev1665-g3f20eb0cd-master; commit `3f20eb0cd22116367c036e6ffe6ace299b38d686`. Any codebase equivalent to this commit that has not applied the fix commit is affected.

Attack Conditions: An attacker supplies a crafted MPEG-2 TS file containing missing sync markers, corrupted PMT descriptor sizes, and conflicting PID assignments. Local access is

must invoke `MP4Box -dash 100 <crafted_file>` or any equivalent DASH segmentation command that triggers PID reconfiguration in the dasher module.

Impact: The use-after-free (READ of size 4 at 316 bytes into a freed 1096-byte heap region) causes process termination, resulting in Denial of Service. Code execution cannot be ruled out:

vulnerabilities can allow an attacker to control freed memory contents and redirect execution flow.

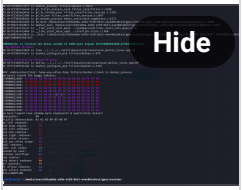
Fix / mitigation status:
The fix ensures the stale PID context pointer in `dasher_configure_pid` is cleared after the region is freed so that `dasher_process` cannot access it.
Users should upgrade to the release containing commit `e6d01820

9ee5f209bc133b` or apply that patch directly.

References

- Issue: github.com/gpac/gpac/issues/33...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/e6...

Credit @sigdevel



#fuzzing

#infosec

#security

...and 9 more

May 30, 2026, 08:19 AM · · We

Last edited
May 30, 08:19 AM

0 boosts · 0 qu