Skip to main content 1
Skip to main navigation 2

P...

sigd...
@si...

Security Advisory: CVE-2025-60465 - Use-After-Free in GPAC MP4Box PID Instance Swap

Processing a crafted media file with MP4Box `-info` can trigger a heap use-after-free in `gf_filter_pid_inst_swap()`, causing a crash and potential code execution.

Summary: The

p()` function in `filter_core/filter_pid.c` does not reset `ctx->pid_inst` to NULL after freeing the PID instance. Subsequent PID configuration and reconfiguration steps can reuse this dangling pointer, leading to access to freed heap memory.

CWE: CWE-416 - Use After Free

Affected Component:
```
filter_core/filter_pid.c:633
```

d_inst_swap()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version: The issue was reproduced on:
```
GPAC version: 2.5-DEV-rev1570-g6208015df-master
Commit: 6208015dff3a6735a26e413c484c714666eb3ea2
```

The MITRE response states that GPAC Project/MP4Box
```

affected. Builds before the fix commit `55b351bd078c950592544ab4c708a613c1725b9b` should be considered affected if they contain the vulnerable PID instance swap path.

Attack Conditions: An attacker supplies a crafted media or MPEG-2 TS input that is processed by MP4Box through the info/import path and triggers filter PID reconfiguration. The issue can be

with:
```
./MP4Box -info 34_gf_filter_pid_inst_swap_filter_core_filter_pid_c_633
```

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

The prepared CVSS vector in

is:
```
AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N
```

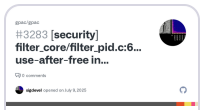
Impact: The immediate observed impact is Denial of Service due to process termination. Because the vulnerability is a heap use-after-free, memory corruption and potential arbitrary code execution are possible.

Fix / mitigation status: The issue was fixed in GPAC

55b351bd078c950592544ab4c708a613c1725b9b
```

Users should update to a GPAC build containing this commit or later. The affected PID instance swap path should clear `ctx->pid_inst` after freeing it and avoid later use of stale PID object pointers.

References:

- Issue: github.com/gpac/gpac/issues/32...
- PoC: github.com
```

- Fix: github.com/gpac/gpac/commit/55...
- CVE record: cve.org/CVERecord?id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)



GitHub

[securi... filter_c...

By **sigdevel**

#fuzzing

#infosec

#security

...and 11 more

Jun 19, 2026, · · We 07:46 PM

0 boosts · **0** qu