sigd...
@si...

Security Advisory: CVE-2025-60471 - Use-After-Free in GPAC MP4Box PID Reconfiguration

Processing a crafted MPEG-2 TS file with MP4Box `-info` can trigger a heap use-after-free in `gf_filter_pid_reconfigure_task_discard()`, causing a crash and potential code execution.

Summary: The `gf_filter_pi

ure_task_discard()` function in `filter_core/filter_pid.c` can access a freed `pid_inst` structure during PID reconfiguration task disposal. When MP4Box processes a specially crafted MPEG-2 Transport Stream file containing broken PMT descriptors, missing packet sync markers, unsupported stream types, and invalid packet data, a PID instance can be freed by `gf_filter_pi

p_delete()` and later accessed in `gf_filter_pid_reconfigure_task_discard()`.

AddressSanitizer reports a `heap-use-after-free` at `filter_core/filter_pid.c:1341`, with a `READ of size 8` from a freed 336-byte heap region.

CWE: CWE-416 - Use After Free

Affected Component:
```
filter_core/filter_pid.c:1341
Function: gf_filter_pi
```

scard()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version: The issue was reproduced on:
```
GPAC version: 2.5-DEV-rev1557-g62714f27c-master
Commit: 62714f27c64a3d1eb7e880f9eed2d38673cb43ce
```

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

affected. Local MITRE data also describes affected GPAC MP4Box 2.4 and earlier, including development branches that contain the vulnerable PID reconfiguration lifecycle handling. Builds before the fix commit `868c6801c226e9964cace54cfd5a759f152780b4` should be considered affected if they contain the vulnerable path.

Attack

supplies a crafted MPEG-2 TS file with corrupted PMT descriptors and invalid packet data. The issue can be reproduced locally with:
```
./MP4Box -info 31_gf_filter_pid_reconfigure_task_discard_filter_core_filter_pid_c_1341
```

No elevated privileges are required. User interaction is required when the victim manually processes

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 a heap use-after-free, memory corruption and potential arbitrary code execution are possible.

Fix / mitigation status: The issue

commit:
```
868c6801c226e9964cace54cfd5a759f152780b4
```
Users should update to a GPAC build containing this commit or later. The affected filter PID reconfiguration path should ensure that PID instance lifetime is valid before task discard logic accesses the object.

References:

- Issue: github.com/gpac/gpac/issues/3

github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/86...
- CVE record: cve.org/CVERecord?id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)

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

Jun 19, 2026, 06:57 PM · We

0 boosts · 0 qu