P...



sigd...
@si...

Security Advisory: CVE-2025-55654 - Use-After-Free in GPAC MP4Box Packet Filtering

Processing a crafted media file with MP4Box `-nhml` export can trigger a heap use-after-free in `gf_filter_pid_get_packet()`, causing a crash and potential memory corruption.

Summary: The `gf_filter_pid_get_pack

Create account Login

function in `filter_core/filter_pid.c` may be called on a `gf_pid_filter_t` object that has already been freed by `gf_filter_pid_del()`. When MP4Box exports a specially crafted file through the `-nhml` path, the file output filter can continue packet processing after the related PID filter object has been released.

AddressSanitizer reports a `heap-use-after-free` at `filter_core/`

Create account Login

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:6792
Function: gf_filter_pid_get_packet()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version: MP4Box versions 2.4 and

Create account Login

according to the prepared CVE/MITRE data. The issue was reproduced on a GPAC build at commit:
```
63eccc33d4a2b731ebb31581ff5673a2c0b13ad4
```
Builds before the fix commit `0ccd2927c7145f5ab0352c5b15f787757b34eb18` should be considered affected if they contain the vulnerable packet filtering/export path.

Attack Conditions: An attacker supplies a

Create account Login

that is processed by MP4Box through the NHML export path. The issue can be reproduced locally with:

```
./MP4Box -nhml trackID 22_data -out /dev/null
```

No elevated privileges are required. User interaction is required when the victim manually processes the malicious file, or an automated media

Create account Login

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 cannot be ruled out.

Fix / mitigation status: The issue was fixed in GPAC commit:
```
0ccd2927c
```

Create account Login

787757b34eb18
```

Users should update to a GPAC build containing this commit or later. The affected filtering path should ensure that a PID filter object remains valid before packet retrieval continues.

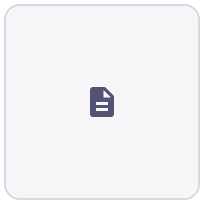
References:

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

Create account Login
```

c/commit/0c…
- CVE record: cve.org/CVERecord?id=CVE-2025-…

Credit Alexander A. Shvedov (@sigdevel)



#fuzzing
#infosec
#security
…and 11 more

Jun 18, 2026, 03:57 AM · · We

0 boosts · 0 qu

Create account Login