P...



sigd...
@si...

Security Advisory: CVE-2025-60478 - Heap Use-After-Free in GPAC Packet Destruction

Processing a crafted MPEG-2 TS input with MP4Box DASH segmentation can trigger a heap use-after-free in `gf_filter_packet_destroy()`.

Summary: Malformed program table data and empty DASH segment state can cause

Create account Login

mishandle packet ownership. The file output and PID packet drop path later destroy a packet object that has already been invalidated.

AddressSanitizer reports `heap-use-after-free` in `filter_core/filter_pck.c`.

CWE: CWE-416 - Use After Free

Affected Component:
```
filter_core/filter_pck.c:678
Function: gf_filter_pa
```

Create account Login

oy()
```

Relevant ASAN stack:

```
gf_filter_packet_destroy filter_core/filter_pck.c:678
gf_filter_packet_destroy filter_core/filter_pck.c:684
gf_filter_pid_drop_packet filter_core/filter_pid.c:7270
fileout_process filters/out_file.c:933
```

Affected Product: MP4Box (GPAC Multimedia Open Source

Create account Login
```

Affected Version:
```
GPAC version: 2.5-DEV-rev1617-g856674b22-master
Commit: 856674b226d6cbe28a941ad223be38194cbf7d37
```

Attack Conditions: An attacker supplies a crafted MPEG-2 TS file that is processed by MP4Box DASH segmentation:

```
./MP4Box -dash 100 47_gf_filter_packet_destroy_filter_core_filter_pck_c_678
```

Create account Login

Impact: The observed impact is Denial of Service. Because the issue is a heap use-after-free, memory corruption risk is also present.

Fix / mitigation status: The MITRE response in the local data records the fix as:

```
c592a144bbe339ee581ca88aaa3247362795b742
```

References:

- CVE: cve.org/CVERecord?

Create account Login

- Issue: github.com/gpac/gpac/issues/33…
- PoC: github.com/sigdevel/pocs/blob/…
- Fix: github.com/gpac/gpac/commit/c5…

Credit Alexander A. Shvedov (@sigdevel)

#fuzzing #infosec #security #afl++ #revers #cybersecurity #bugbounty #vulnerability #opensource #linux #cve #advisory #gpac

Oct

Create account Login

01:47
PM

0 boosts · **0** qu

Create account Login