sigd...
@si...

Security Advisory: CVE-2025-55664 - Heap-based Buffer Overflow in GPAC/MP4 Box

Processing a crafted MPEG-2 Transport Stream file with corrupted packet structures triggers a heap buffer overflow in `m2tsdmx_send_packet`, causing MP4Box to crash and potentially enabling arbitrary code execution.

Summary: The `m2tsdmx_send_packet` function in `filters/dmx_m2ts.c` performs a `memcpy` whose size argument is derived from stream-controlled data without validation. A crafted MPEG-2 TS file with missing sync markers, corrupted PMT descriptors, and PID conflicts can cause the size to wrap to 4294967295 (0xFFFFFFFF), triggering a `memcpy`

and writes 4 GB of heap memory starting one byte past the end of a 183-byte allocated region.

CWE: CWE-122 - Heap-based Buffer Overflow

Affected Component

```
filters/dmx_m2ts.c:916
Function: m2tsdmx_send_packet()
```

Affected Product: MP4Box (GPAC Multimedia Open

Affected Version: 2.5-DEV-rev1644-g8e3b5e1dd-master; commit `8e3b5e1dde7b9ea041dbdc14456a5bb74a9851ea`. Any codebase equivalent to this commit that has not applied the fix commit is affected.

Attack Conditions: An attacker supplies a specially crafted MPEG-2 TS file containing missing sync markers (0x47), corrupted PMT descriptor

PID assignments. Local access is required; the victim must invoke `MP4Box -dash 100 <crafted_file>` or any equivalent DASH segmentation command that triggers the MPEG-2 TS demuxer processing path.

Impact: The heap buffer overflow (READ of size 4294967295, 1 byte past end of a 183-byte heap region) results in process termination

Service. Due to the write-capable nature of the oversized `memcpy`, arbitrary code execution cannot be ruled out.

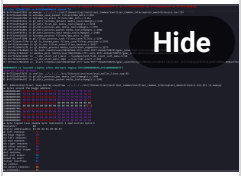
Fix / mitigation status: The fix adds size validation before the `memcpy` call in `m2tsdmx_send_packet` to reject stream-supplied sizes that exceed the allocated buffer. Users should upgrade to the release containing commit `9bd6a72c

afc7658dabd26` 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/9b...

Credit @sigdevel



#fuzzing

#infosec

#security

...and 9 more

May 29, 2026, 06:20 PM · · We