

sigd...
@si...

Security Advisory: CVE-2025-60480 - Heap Buffer Overflow in GPAC MP4Box AC-4 Alternative Info Parsing

A heap buffer overflow vulnerability exists in GPAC MP4Box when processing a crafted AC-4 stream. The issue occurs in `gf_odf_ac4_cfg_alternative_info()` in `odf/descri

Create account Login

triggered by running MP4Box with the `-info` option on a malformed input file.

Summary: AddressSanitizer confirms a heap-buffer-overflow at `odf/descriptors.c:1899`. The vulnerable code reads 1 byte past the end of an allocated buffer due to insufficient bounds checking of AC-4 `alt_group_id` array indexes.

The crafted AC-4 stream reaches

Create account Login

generation and causes `gf_odf_ac4_cfg_alternative_info()` to access `alt_group_id` data outside the bounds of an allocated buffer. The allocation originates while parsing the raw AC-4 frame, and the out-of-bounds read occurs later while writing AC-4 descriptor information.

Relevant AddressSanitizer trace:

```
==1847116
==ERROR:
```

Create account Login

heap-buffer-overflow on address 0x518000000f90 READ of size 1 at 0x518000000f90 thread T0
#0 0x... in gf_odf_ac4_cfg_alternative_info odf/descriptors.c:1899
#1 0x... in gf_odf_ac4_cfg_presentation_v1_dsi odf/descriptors.c:2103
#2 0x... in gf_odf_ac4_cfg_dsi_v1 odf/descriptors.c:2233
#3 0x... in gf_odf_ac4_cfg_write

Create account Login

odf/descriptors.c:2281
#4 0x... in gf_odf_ac4_cfg_write odf/descriptors.c:2288
#5 0x... in ac4dmx_check_pid filters/reframe_ac4.c:238
#6 0x... in ac4dmx_process filters/reframe_ac4.c:403
#7 0x... in gf_filter_process_task filter_core/filter.c:3187
#8 0x... in gf_fs_thread_proc filter_core/filter_session.c:2421
#9 0x... in gf_fs_run

Create account Login

ilter_session.c:2728
#10 0x... in gf_media_import media_tools/media_import.c:1278
#11 0x... in convert_file_info applications/mp4box/fileimport.c:131
#12 0x... in mp4box_main applications/mp4box/mp4box.c:6520

0x518000000f90 is located 0 bytes after 784-byte region [0x518000000c80,0x518000000f90) allocated by thread

Create account Login

in malloc
#1 0x... in gf_ac4_raw_frame media_tools/av_parsers.c:15916
#2 0x... in gf_ac4_parser_bs media_tools/av_parsers.c:16113

SUMMARY: AddressSanitizer: heap-buffer-overflow odf/descriptors.c:1899 in gf_odf_ac4_cfg_alternative_info
```

CWE: CWE-122 - Heap-based Buffer Overflow

Affected Componen

Create account Login
```

odf/descriptors.c:1899
Function: gf_odf_ac4_cfg_alternative_info()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version:
```
2.5-DEV-rev1593-gfe88c3545-master
Commit: fe88c3545aadd597b250ccf23271d5d3de50ccc8
```

Attack Conditions: An attacker supplies a crafted input file

Create account Login
```

by MP4Box. The issue can be reproduced locally with:
```
./MP4Box -info 44_gf_odf_ac4_cfg_alternative_info_odf_descriptors_c_1899
```

Attack vector: local crafted AC-4 file processed by MP4Box User interaction: required

Impact: denial of service via application crash; local MITRE data also identifies potential arbitrary

Create account Login

execution risk

Fix / mitigation status:
The issue was fixed in GPAC commit:
```
e02d1fd24cdc26acb1b236ab38b3832cffcae21b
```
Users should update to a GPAC build containing this commit or later.

References:

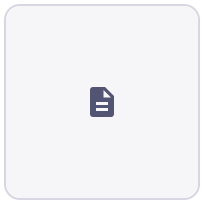
- Issue: github.com/gpac/gpac/issues/32...
- Fix: github.com/gpac/gpac/commit/e0...

Create account Login

/sigdevel/pocs/blob/... - CVE: cve.org/CVERecord?id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)

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



Oct 17, 2026, · · We 01:30

Create account Login

Create account Login