

sigd...
@si...

Security Advisory: CVE-2025-60475 - Global Buffer Overflow in GPAC MP4Box AC-4 Parser

A global buffer overflow vulnerability exists in GPAC MP4Box when processing a crafted AC-4 audio stream. The issue occurs in `gf_ac4_parser_bs()` in `media_tools/av_parsers.c` and can be

Create account Login

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

Summary: AddressSanitizer confirms an out-of-bounds read at `media_tools/av_parsers.c:16140`. The parser accesses `AC4_SAMPLE_DELTA_TABLE_48` with an out-of-bounds index, causing a 4-byte read past the global array boundary. The AC-4 parser reads index values from the input

Create account Login

them to access the global `AC4_SAMPLE_DELTA_TABLE_48` array. The vulnerable path does not properly validate the index before accessing the table. A crafted AC-4 stream can therefore cause a read just past the end of the global array.

CWE: CWE-125 - Out-of-bounds Read

Affected Component:
```
media_tools/av_parse

Create account Login
```

gf_ac4_parser_bs()
```

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 that is processed by MP4Box. The issue

Create account Login
```

locally with:
```
./MP4Box -info 40_gf_ac4_parser_bs_media_tools_av_parsers_c_16140
```

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

Impact: denial of service via application crash; local triage notes also identify potential information disclosure or code execution risk

Create account Login

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

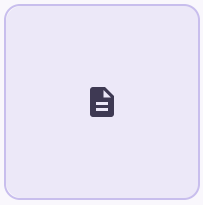
References:

- Issue: github.com/gpac/gpac/issues/32...
- Fix: github.com/gpac/gpac/commit/e0...
- PoC: github.com/sigdevel/pocs/blob/...
- CVE

Create account Login

ERecord?id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)



Oct 17, 2026, · · We 12:55 PM

0 boosts · **0** qu

Create account Login