P...

sigd...
@si...

Security Advisory: CVE-2025-60473 - NULL Pointer Dereference in GPAC MP4Box Filter Parent Chain

Processing a crafted media file with MP4Box `-info` can trigger a NULL pointer dereference in `gf_filter_in_parent_chain()`, causing a Denial of Service.

Summary: The `gf_filter_in

ain()` function in `filter_core/filter_pid.c` does not sufficiently validate a parent filter pointer before dereferencing it. When MP4Box processes a specially crafted media file with malformed MPEG-2 TS data and a corrupted PID/filter chain, the vulnerable path can attempt to read from address `0x000000000008`.

CWE: CWE-476 - NULL Pointer Dereference

t:
```
filter_core/filter_pid.c:2145
Function: gf_filter_in_parent_chain()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version: The issue was reproduced on:
```
GPAC version: 2.5-DEV-rev1570-g6208015df-master
Commit: 6208015dff3a6735a26e413c484c714666eb3ea2
```

The MITRE response states that GPAC Project/MP4Box before `26.02.0` is affected. Builds before the fix commit `b8d80b44718de10b101e1d7fc17c84d69feb092e` should be considered affected if they contain the vulnerable filter parent-chain validation path.

Attack Conditions: An attacker supplies a crafted media file with malformed MPEG-2 TS packet

PID/filter chain. The issue can be reproduced locally with:
```
./MP4Box -info 36_gf_filter_in_parent_chain_filter_core_filter_pid_c_2145
```

No elevated privileges are required. User interaction is required when the victim manually processes the malicious file, or an automated media workflow invokes MP4Box on attacker-

The prepared CVSS vector:
```
AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
```

Impact: The immediate observed impact is Denial of Service due to process termination. The local MITRE/BDU data also notes potential arbitrary code execution, although the available ASAN evidence shows a NULL pointer dereference crash.

status:
The issue was fixed in GPAC commit:
```
b8d80b44718de10b101e1d7fc17c84d69feb092e
```

Users should update to a GPAC build containing this commit or later. The affected filter graph code should validate parent filter pointers before dereferencing them during PID initialization.

References:

- Issue:

c/issues/32...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/b8...
- CVE record: cve.org/CVERecord?id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)

#fuzzing
#infosec
#security
...and 11 more

Jun 20, 2026, · · We 04:09 AM

Last edited