Skip to main content 1
Skip to main navigation 2

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:

_parent_chain()` 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 Dereferenc e

Affected Component:
```
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: 6208015dff3a6735a26e413c484
```

3ea2
```

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
```

packet data and a corrupted 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

attacker-controlled input.

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

dereferenc
e crash.

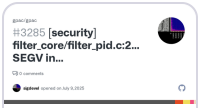
Fix /
mitigation
status:
The issue
was fixed
in GPAC
commit:
```
b8d80b447
18de10b10
1e1d7fc17
c84d69feb
092e
```

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

References:

- Issue: github.com/gpac/gpac/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)



GitHub

[securi... filter_c...

By **sigdevel**

#fuzzing

...and 11 more

Jun 20, 2026, 04:09 AM · · We

Last edited **Jun 20, 04:10 AM**

0 boosts · **0** qu

Create account Login