

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
60466 -
Expired
Pointer
Dereferenc
e in GPAC
MP4Box
Packet
Retrieval

Processing
a crafted
media file
with
MP4Box ` -
info` can
trigger an
expired
pointer
dereferenc
e in
`gf_filter_pi
d_get_pack
et()`,
causing a
heap use-
after-free
crash and
potential
code
execution.

Create account

Login



Summary:
The ``gf_filter_pid_get_packet()`` function in ``filter_core/filter_pid.c`` may operate on an invalidated Packet ID (PID) object after it has been freed by ``gf_filter_pid_del()``. When MP4Box processes a specially crafted media file through the filter graph, the ``inspect`` filter can request packets from a stale PID object, leading to access to freed heap memory.

[Create account](#)[Login](#)

CWE:
CWE-825 -
Expired
Pointer
Dereferenc
e

Affected
Componen
t:
...

filter_core/f
ilter_pid.c:6
827
Function:
gf_filter_pi
d_get_pack
et()
...

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
The issue
was
reproduced
on:
...

GPAC
version:
2.5-DEV-

f-master
Commit:
6208015df
f3a6735a2
6e413c484
c714666eb
3ea2
...

The MITRE response states that GPAC Project/MP 4Box before `26.02.0` is affected. Builds before the fix commit `4a7ea06d d1b2cc65f e0dabc601 89eb6bc81 4f7bb` should be considered affected if they contain the vulnerable PID packet retrieval path.

Attack Conditions:
An attacker

media file
that is
processed
by MP4Box
through the
info/import
path and
drives the
inspect/filt
er pipeline
through
PID
deletion
and packet
retrieval
paths. The
issue can
be
reproduced
locally
with:

...

```
./MP4Box -  
info  
35_gf_filter  
_pid_get_p  
acket_filter  
_core_filter  
_pid_c_682  
7  
...
```

No
elevated
privileges
are
required.
User
interaction

[Create account](#)[Login](#)

victim manually processes the malicious file, or an automated media workflow invokes MP4Box on attacker-controlled input.

The prepared CVSS vector in the local BDU data is:
...

AV:L/AC:L/
PR:N/UI:R/
S:U/C:L/I:H
/A:N
...

Impact:
The immediate observed impact is Denial of Service due to process termination . Because

y is a heap use-after-free / expired pointer dereference, memory corruption and potential arbitrary code execution are possible.

Fix / mitigation status:
The issue was fixed in GPAC commit:
...

4a7ea06dd
1b2cc65fe
0dabc6018
9eb6bc814
f7bb
...

Users should update to a GPAC build containing this commit or later. The

ignore tasks when PID or filter objects have been removed or finalized, preventing stale object use.

References

- Issue: github.com/gpac/gpac/issues/32...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/4a...
- CVE record: cve.org/CVERecord?id=CVE-2025-...

Credit
Alexander
A. Shvedov
(@sigdevel

[Create account](#)[Login](#)



#fuzzing

#infosec

#security

...and 11 more

Jun
20,
2026, · 🌐 · We
03:52
AM

0 boosts · 0 qu



Create account

Login