

← P... 🔒



sigd...
@si...

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

Processing
a crafted
media file
with
MP4Box ` -
info` can
trigger a
NULL
pointer
dereferenc
e in
`gf_filter_in
_parent_ch
ain()`,
causing a
Denial of
Service.

Summary:
The
`gf_filter_in

Create account

Login



ain()
function in
`filter_core/
filter_pid.c`
does not
sufficiently
validate a
parent filter
pointer
before
dereferenci
ng 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
`0x000000
000008`.

CWE:
CWE-476 -
NULL
Pointer
Dereferenc
e

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

t:
...

filter_core/f
ilter_pid.c:2
145
Function:
gf_filter_in_
parent_chai
n()
...

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

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

GPAC
version:
2.5-DEV-
rev1570-
g6208015d
f-master
Commit:
6208015df
f3a6735a2
6e413c484
c714666eb
3ea2

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

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

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

PID/filter
chain. The
issue can
be
reproduced
locally
with:

...

```
./MP4Box -  
info  
36_gf_filter  
_in_parent_  
chain_filter  
_core_filter  
_pid_c_214  
5
```

...

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-

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

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/BD
U data also
notes
potential
arbitrary
code
execution,
although
the
available
ASAN
evidence
shows a
NULL
pointer
dereferenc
e crash.

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

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.

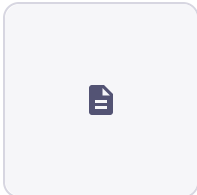
References
:

- Issue:

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

[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

0 boosts · 0 qu



Create account

Login