

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
60465 -
Use-After-
Free in
GPAC
MP4Box
PID
Instance
Swap

Processing
a crafted
media file
with
MP4Box ` -
info` can
trigger a
heap use-
after-free in
`gf_filter_pi
d_inst_swa
p()`,
causing a
crash and
potential
code
execution.

Summary:
The
`gf_filter_pi
d_inst_swa

Create account

Login



function in
`filter_core/
filter_pid.c`
does not
reset `ctx-
>pid_inst`
to NULL
after
freeing the
PID
instance.
Subsequen
t PID
configurati
on and
reconfigura
tion steps
can reuse
this
dangling
pointer,
leading to
access to
freed heap
memory.

CWE:
CWE-416 -
Use After
Free

Affected
Component:
...

filter_core/f
ilter_pid.c:6
33
Function:

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

p()
'''

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
'''

The MITRE
response
states that
GPAC
Project/MP
4Box
before

Builds
before the
fix commit
`55b351bd
078c95059
2544ab4c7
08a613c17
25b9b`
should be
considered
affected if
they
contain the
vulnerable
PID
instance
swap path.

Attack
Conditions:
An attacker
supplies a
crafted
media or
MPEG-2 TS
input that
is
processed
by MP4Box
through the
info/import
path and
triggers
filter PID
reconfigura
tion. The
issue can
be
reproduced

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

```
```
```

```
./MP4Box -
info
34_gf_filter
_pid_inst_s
wap_filter_
core_filter_
pid_c_633
```
```

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-controlled input.

The prepared CVSS vector in the local

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

```

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
the
vulnerabilit
y is a heap
use-after-
free,
memory
corruption
and
potential
arbitrary
code
execution
are
possible.

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

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

```
78c950592
544ab4c70
8a613c172
5b9b
```
```

Users should update to a GPAC build containing this commit or later. The affected PID instance swap path should clear `ctx->pid\_inst` after freeing it and avoid later use of stale PID object pointers.

References  
:

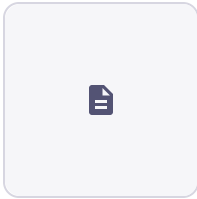
- Issue:  
[github.com/gpac/gpac/issues/32](https://github.com/gpac/gpac/issues/32)...

- PoC:  
[github.com/sigdevel/p](https://github.com/sigdevel/poc)

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

[github.com](#)  
[/gpac/gpac/commit/55...](#)  
- CVE  
record:  
[cve.org/CVERecord?id=CVE-2025-...](#)

Credit  
Alexander  
A. Shvedov  
([@sigdevel](#))



- #fuzzing
- #infosec
- #security

...and 11 more

Jun  
19,  
2026, · · We  
07:46  
PM

0 boosts · 0 qu

