



sigd...
@si...

Security
Advisory:
CVE-2025-
60471 -
Use-After-
Free in
GPAC
MP4Box
PID
Reconfigur
ation

Processing
a crafted
MPEG-2 TS
file with
MP4Box ` -
info` can
trigger a
heap use-
after-free in
`gf_filter_pi
d_reconfig
ure_task_di
scard()`,
causing a
crash and
potential
code
execution.

Summary:
The
`gf_filter_pi

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

ure_task_di
scard()
function in
`filter_core/
filter_pid.c`
can access
a freed
`pid\_inst`
structure
during PID
reconfigura
tion task
disposal.
When
MP4Box
processes
a specially
crafted
MPEG-2
Transport
Stream file
containing
broken
PMT
descriptors
, missing
packet
sync
markers,
unsupporte
d stream
types, and
invalid
packet
data, a PID
instance
can be
freed by
`af_filter_pi

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

```
p_delete()
and later
accessed
in
`gf_filter_pi
d_reconfig
ure_task_di
scard()`.
```

AddressSanitizer reports a `heap-use-after-free` at
`filter_core/
filter_pid.c:
1341`, with
a `READ` of
size 8`
from a
freed 336-
byte heap
region.

CWE:
CWE-416 -
Use After
Free

Affected
Component:
...

filter_core/f
ilter_pid.c:1
341

Function:
gf_filter_pi

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

scard()
...

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

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

GPAC
version:
2.5-DEV-
rev1557-
g62714f27
c-master
Commit:
62714f27c
64a3d1eb7
e880f9eed
2d38673cb
43ce
...

The MITRE
response
states that
GPAC
Project/MP
4Box

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

affected.
Local
MITRE data
also
describes
affected
GPAC
MP4Box
2.4 and
earlier,
including
developme
nt
branches
that
contain the
vulnerable
PID
reconfigura
tion
lifecycle
handling.
Builds
before the
fix commit
`868c6801
c226e9964
cace54cf
5a759f152
780b4`
should be
considered
affected if
they
contain the
vulnerable
path.

Attack

Create account

Login

supplies a crafted MPEG-2 TS file with corrupted PMT descriptors and invalid packet data. The issue can be reproduced locally with:

```
...  
./MP4Box -  
info  
31_gf_filter  
_pid_reconf  
igure_task_  
discard_filt  
er_core_filt  
er_pid_c_1  
341  
...
```

No elevated privileges are required. User interaction is required when the victim manually processes

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

file, or an automated media workflow invokes MP4Box on attacker-controlled input.

Impact:
The immediate observed impact is Denial of Service due to process termination . Because the vulnerability is a heap use-after-free, memory corruption and potential arbitrary code execution are possible.

Fix / mitigation status:
The issue

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

commit:

...

868c6801c
226e9964c
ace54cfd5
a759f1527
80b4

...

Users should update to a GPAC build containing this commit or later. The affected filter PID reconfiguration path should ensure that PID instance lifetime is valid before task discard logic accesses the object.

References
:

- Issue:
github.com/gpac/gpac/issues/3

Create account

Login

[github.com](#)
[/sigdevel/p](#)
[ocs/blob/...](#)

- Fix:

[github.com](#)
[/gpac/gpa](#)
[c/commit/](#)
[86...](#)

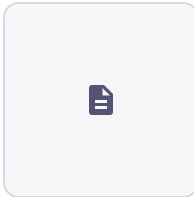
- CVE

record:

[cve.org/CV](#)
[ERecord?](#)
[id=CVE-](#)
[2025-...](#)

Credit

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



[#fuzzing](#)

[#infosec](#)

[#security](#)

...and 11 more

Jun
19,
2026, · · We
06:57
PM

0 boosts · 0 qu



Create account

Login