

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
60467 -
Use-After-
Free in
GPAC
MP4Box
PID Swap
Delete Task

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

Summary:
The
`gf_filter_pi
d_inst_swa

Create account

Login



sk() function in ``filter_core/filter_pid.c`` can access a ``GF_FilterPidInstance`` object after it has already been freed by ``gf_filter_pid_inst_swap_delete()``. Crafted input that exercises filter reconfiguration and deferred teardown paths can cause the scheduler to process a delete task with a stale pointer.

AddressSanitizer reports a ``heap-use-after-free`` at

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

574`, with a
`READ of
size 4`
from a
previously
freed 336-
byte heap
region.

CWE:
CWE-416 -
Use After
Free

Affected
Component:
...

filter_core/f
ilter_pid.c:5
74
Function:
gf_filter_pi
d_inst_swa
p_delete_ta
sk()
...

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:

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

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
`26.02.0` is
affected.
Builds
before the
fix commit
`976dacf65
cb6986a4e
4f350fb8d
3ed0a17dc
3a77`
should be
considered
affected if
they
contain the

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

PID swap
delete task
path.

Attack
Conditions:
An attacker
supplies a
crafted
media file
or filter
graph input
that is
processed
by MP4Box
through the
info/import
path and
triggers
PID
reconfigura
tion and
deferred
teardown.
The issue
can be
reproduced
locally
with:

```
...  
./MP4Box -  
info  
37_gf_filter  
_pid_inst_s  
wap_delete  
_task_filter  
_core_filter  
_pid_c_574  
...
```

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

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:
...

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

Impact:
The immediate observed

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

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 was fixed in GPAC commit: ...

976dacf65
cb6986a4e
4f350fb8d
3ed0a17dc
3a77
...

Users should update to a GPAC build containing

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

later. The affected deferred task path should ensure that ``GF_FilterPidInstance`` lifetime remains valid before a scheduled delete task accesses it.

References

:

- Issue:

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

- PoC:

[github.com
/sigdevel/p
ocs/blob/...](https://github.com/sigdevel/pocs/blob/...)

- Fix:

[github.com
/gpac/gpac/
commit/97...](https://github.com/gpac/gpac/commit/97...)

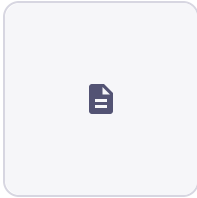
- CVE
record:

[cve.org/CV
ERecord?
id=CVE-](https://cve.org/CVERecord?id=CVE-)

Create account

Login

Credit
Alexander
A. Shvedov
(@sigdevel
)



- #fuzzing
- #infosec
- #security

...and 11 more

Jun
20,
2026, · 🌐 · We
04:21
AM

0 boosts · 0 qu

