

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
55647 -
Integer
Overflow in
GPAC
MP4Box
PSSH
Handling

Processing
a crafted
MP4 file
with
malformed
Protection
System
Specific
Header
(PSSH)
data can
trigger an
integer
overflow
and
uncontrolle
d
allocation
in
`mp4_mux_
cenc_insert_
_pssh()`

Create account

Login



Service through memory exhaustion.

Summary:
The ``mp4_mux_cenc_insert_pssh()`` function in ``filters/mux_isom.c`` does not sufficiently validate PSSH sizes before allocating memory. A crafted MP4 file can set PSSH-related fields such as ``kid_count`` or ``dataSize`` to very large values. This can overflow the buffer size calculation and cause

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

very large
allocation
during
DASH/mux
processing
.

AddressSanitizer
reports an
out-of-
memory
condition
at
`filters/mux
_isom.c:43
26`, where
`realloc()`
attempts to
allocate
`0xe40000
100` bytes.

CWE:
CWE-190 -
Integer
Overflow or
Wraparound

Affected
Component:
...

filters/mux
_isom.c:43
26

Function:
mp4_mux_

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

```
_pssh()  
...  

```

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
MP4Box
versions
2.4 and
earlier are
affected
according
to the
prepared
CVE/MITR
E data. The
issue was
reproduced
on a GPAC
build at
commit:
...

```
e95f3064d  
846e46062  
76fff111e0  
f97df1576  
a04  
...  

```

Builds
before the
fix commit

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

7ba06618b
ff9d58714
1792`
should be
considered
affected if
they
contain the
vulnerable
PSSH
allocation
path.

Attack
Conditions:
An attacker
supplies a
crafted
MP4 file
containing
malformed
PSSH/CEN
C
metadata.
The issue
can be
reproduced
locally
with:
...

./MP4Box -
dash
10000
./15_poc.m
p4
...

No
elevated
privileges

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

User interaction is required when the victim manually processes the malicious MP4 file, or an automated media workflow invokes MP4Box on attacker-controlled input.

Impact:
The immediate observed impact is Denial of Service due to memory exhaustion and process termination . Because the root cause is an integer overflow in allocation-size

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

corruption
and
potential
arbitrary
code
execution
cannot be
ruled out.

Fix /
mitigation
status:

The issue
was fixed
in GPAC
commit:
...

2a1f63853
4cddf511a
7ba06618b
ff9d58714
1792
...

References

:

- Issue:

[github.com
/gpac/gpa
c/issues/3
2...](https://github.com/gpac/gpac/issues/32)

- PoC:

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

- Fix:

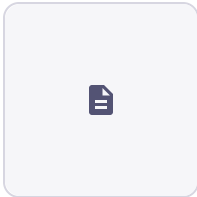
[github.com
/gpac/gpa
c/commit/](https://github.com/gpac/gpac/commit/)

Create account

Login

record:
[cve.org/CVERecord?id=CVE-2025-...](#)

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



- #fuzzing
- #infosec
- #security

...and 11 more

Jun 12, 2026, · · We 11:02 AM

Last edited
Jun 16, 06:16 PM

1 boost · 0 quotes



EN

[@sigdevel](#)
Hello

Create account

Login

add
direc
t
refer
ence
s to
the
CVE
too.
Right
now
there
is
only
this
Mast
odon
toot.
Plea
se
add
direc
t
refer
ence
s
also
to
the
"Issu
e",
"PoC
" and
"Fix"
you
have
shar
ed in
this
too.

Than
ks!

↩ 0

Create account

Login