



sigd...
@si...

Security
Advisory:
CVE-2025-
55645 -
Heap
Buffer
Overflow in
GPAC
MP4Box
PSSH Copy

Processing
a crafted
MP4 file
with
malformed
PSSH data
can trigger
a heap
buffer
overflow in
`gf_cenc_s
et_pssh()`,
causing a
crash and
potential
memory
disclosure
or memory
corruption
impact.

Summary:
The

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

et_pssh() function in `isomedia/drm\_sample.c` does not sufficiently validate the size of PSSH data before copying it into a heap buffer. A crafted MP4 file can declare an oversized PSSH payload, causing MP4Box to copy a very large amount of data from a 512-byte heap allocation during DASH/CENC processing.

CWE:
CWE-120 -
Buffer

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

Checking
Size of
Input

Affected
Component:
...

isomedia/d
rm_sample
.c:982
Function:
gf_cenc_se
t_pssh()
...

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
MP4Box
versions
2.4 and
earlier are
affected
according
to the
prepared
CVE/MITRE
data. The
local
MITRE

Create account

Login

`2.5-DEV-
rev228-
g11067ea9
2-master`
as
affected.
The issue
was
reproduced
on a GPAC
build at
commit:

...

e95f3064d
846e46062
76fff111e0
f97df1576
a04

...

Builds
before the
fix commit
`df0c81722
847238659
a6beb0fea
b2c1ecd05
c020`
should be
considered
affected if
they
contain the
vulnerable
PSSH copy
path.

Attack

Create account

Login

supplies a crafted MP4 file containing malformed PSSH/CENC metadata with an oversized declared payload. The issue can be reproduced locally with:

...

```
./MP4Box -dash 10000 ./16_poc.mp4
```

...

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

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

automated
media
workflow
invokes
MP4Box on
attacker-
controlled
input.

Impact:
The
immediate
observed
impact is
Denial of
Service due
to process
termination
. Because
the bug
performs
an
oversized
heap read
during
`memcpy()`
,
informatio
n
disclosure
may be
possible.
Memory
corruption
and
potential
arbitrary
code
execution

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

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

...

df0c81722
847238659
a6beb0fea
b2c1ecd05
c020
...

Users
should
update to a
GPAC build
containing
this
commit or
later. The
affected
code
should
validate
PSSH
payload
sizes and
destination
buffer
capacity
before
copying
PSSH data.

References

Create account

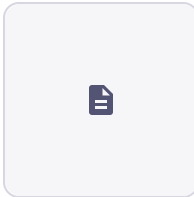
Login

[github.com](#)
[/gpac/gpac/issues/32...](#)

- PoC:
[github.com](#)
[/sigdevel/pocs/blob/...](#)

- Fix:
[github.com](#)
[/gpac/gpac/commit/df...](#)

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



[#fuzzing](#)

[#infosec](#)

[#security](#)

...and 11 more

Jun
12,
2026, ·  · We
11:04
AM

Last edited
Jun 12, 11:23 AM

1 boost · 0 quotes

Create account

Login



EN  

@sig
devel

Hello
,
pleas
e
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

Create account

Login

this
too.

Than
ks!

↩ 0

Create account

Login