

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
55644 -
Use-After-
Free in
GPAC
MP4Box

Processing
a crafted
MP4 file
with invalid
BIFS
GlobalQua
ntizer
commands
causes
gf_node_ge
t_tag() to
access a
freed 192-
byte
Quantizatio
nParamete
r node at
scenegrap
h/base_sce
negraph.c:
1263,
resulting in
a heap use-
after-free

Create account

Login



Summary:
During MPEG-4 BIFS scene decoding, BM_ParseGlobalQuantizer() in bifs/memory_decoder.c first calls gf_node_unregister() at line 176 to release a QuantizationParameter node, freeing the 192-byte heap region. Without clearing the stale pointer, the function then calls gf_node_get_tag() on the same address at line 181, performing a READ of 8 bytes at offset 0 into the freed

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

crafted MP4 containing invalid GlobalQuantizer BIFS commands, corrupted ODF descriptors, and malformed box types (PEC1808, fre) reliably triggers this free-then-use sequence through the -svg dump path.

CWE:
CWE-416 - Use After Free

Affected Component:
...

scenegraph/base_scenegraph.c:
1263
...

Affected

Create account

Login

(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
MP4Box
2.4 and
earlier;
tested at
commit
f5b7cdc63
a7f326904
0778c5431
a8f6c310b
c9f3

Attack
Conditions:
An attacker
supplies a
locally
accessible
crafted
MP4 file
embedding
invalid BIFS
scene data.
The victim
runs
MP4Box -
svg on the
file to
trigger
BIFS scene
parsing. No
elevated

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

are
required.

Impact:
The use-
after-free
causes a
fatal crash
(Denial of
Service).
Use-after-
free
vulnerabiliti
es can
allow
attackers
to control
freed heap
memory
contents
and
potentially
redirect
execution
flow; code
execution
cannot be
excluded.

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

63eccc33d
4a2b731eb

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

3ad4

...

Users should update to a GPAC build containing this commit or later.

References

:

- Issue:

github.com/gpac/gpac/issues/32...

- PoC:

github.com/sigdevel/pocs/blob/...

- Fix:

github.com/gpac/gpac/commit/63...

- CVE record:

cve.org/CVERecord?id=CVE-2025-...

Credit:

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

Create account

Login



#fuzzing

#infosec

#security

...and 11 more

Jun
12,
2026, · 🌐 · We
11:12
AM

Last edited
Jun 16, 06:14
PM

0 boosts · 0 qu



EN 🗨 🌙

@sig
devel
why
are
you
posti
ng
this
on
#afl
hash
tag

🔍 1

EN 🗨 🗨 🌙

@ak
ent

Create account

Login

usin
g the
AFL
tool
([aflpl
us.pl
us/](#))
This
has
nothi
ng to
do
with
Austr
alian
footb
all;
I'll
rena
me it
to
clarif
y =)

↩ 1

 EN  

[@sig
devel](#)
thx!
all
good

↩ 0

 EN  

[@sig](#)

Create account

Login

,
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
ed in
this
too.

Than
ks!

Create account

Login



EN  

@iamleo
t
Thank you for your feedback!
I have also added the "CVE record" key-value pair to the Advisory-template, with a link to the reserved/published vulnerability report.
Future entries

Create account

Login

generated in the new format

1



EN

@sigdevel

Can you please also contact the CNA where you requested such CVEs and update also the existing one?

This make work of folks follo

Create account

Login

king/
man
agin
g
CVEs
bette
r.

↩ 1

 EN  

@iamleo
t Of
cour
se,
requ
ests
to
add
links
were
sent
in
the
follo
w-up
emai
l
regar
ding
the
publi
catio
n. I
notic
ed
that
the
origi
nal
links
were
missi
ng

Create account

Login

e
CVE
entri
es,
but
my
proc
ess
hasn'
t
chan
ged
rece
ntly.
full-
cont
ext:
[cve.o](#)
[rg/C](#)
[VERe](#)
[cord](#)
[?](#)
[id=C](#)
[VE-](#)
[2025](#)
-...
trunc
ated:
[cve.o](#)
[rg/C](#)
[VERe](#)
[cord](#)
[?](#)
[id=C](#)
[VE-](#)
[2025](#)
-...
↩ 1



EN  

@sig
devel
Than
ks!

Create account

Login

-604
85,
with
all
the
refer
ence
s is a
good
exa

—

|

|