

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
60474 -
Heap
Buffer
Overflow in
GPAC
MP4Box
Media
Import

A heap
buffer
overflow
vulnerabilit
y exists in
GPAC
MP4Box
when
processing
a crafted
media file
with the `
info`
option. The
issue
occurs in
`gf_media_i
mport()` in
`media_too
ls/media_i
mport.c`

Create account

Login



by
supplying a
malformed
input file to
MP4Box.

Summary:
AddressSanitizer
confirms
an out-of-
bounds
read at
`media\_tools/media\_import.c:1297`. The
vulnerable
code reads
1 byte at
offset `[1]`
from a 1-
byte heap
buffer
allocated
from an
empty
string via
`strdup("")`,
where only
offset `[0]`
is valid.
The crafted
input
reaches
MP4Box
media
import
handling

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

import() to access memory immediately after a 1-byte heap allocation. The allocation originates from property handling for an empty string and is later read out of bounds during media import processing.

CWE:
CWE-122 -
Heap-
based
Buffer
Overflow

Affected
Component:
...

media_tools/media_import.c:12

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

gf_media_i
mport()
...

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
...

2.5-DEV-
rev1570-
g6208015d
f-master
Commit:
6208015df
f3a6735a2
6e413c484
c714666eb
3ea2
...

Attack
Conditions:
An attacker
supplies a
crafted
input file
that is
processed
by
MP4Box.
The issue

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

locally

with:

'''

./MP4Box -

info

38_gf_medi

a_import_

media_tool

s_media_i

mport_c_1

297

'''

The

prepared

CVSS

vector:

'''

CVSS:3.1/

AV:L/AC:L/

PR:N/UI:R/

S:U/C:N/I:N

/A:H

'''

Impact:

denial of

service via

application

crash; local

triage

notes also

identify

potential

code

execution

risk

Fix /

Create account

Login

The issue
was fixed
in GPAC
commit:
...

bd7fd6be5
46e0cd9e5
99c6b262c
338c5f2ec
ec5c
...

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

References
:

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

- Fix:
[github.com
/gpac/gpa
c/commit/
bd...](https://github.com/gpac/gpac/commit/bd7fd6be546e0cd9e599c6b262c338c5f2ec5c)

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

- CVE
record:
cve.org/CV

Create account

Login

id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)

#fuzzing

#infosec

#security

...and 11 more

Jun 20, 2026, · 🌐 · We

04:33 AM

0 boosts · 0 qu

↩️ ↺ ⭐ 📌 ...

Create accountLogin

https://infosec.exchange/@sigdevel/1167805667999525927/7