

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
60495 -
NULL
Pointer
Dereferenc
e in
GPAC/MP4
Box

Processing
a crafted
MP4 file
with an
inconsisten
t video
sample
entry
triggers a
NULL
pointer
dereferenc
e in
`gf_media_
get_color_i
nfo`,
causing
MP4Box to
crash.

Summary:
The
`gf_media_

Create account

Login



nfo`
function in
`media\_tools/isom\_tools.c`
inspects
codec-specific
boxes
nested
inside a
video
sample
entry.
When a
sample
entry type
(e.g.,
`v210`)
unexpectedly
contains
an
unrelated
box (e.g.,
an `avcC`
AVC
Decoder
Configuration
Box),
the
function
dereferences a near-
NULL
pointer
(READ at
address
0x00000000

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

NULL-check is performed before the dereference, and the process terminates with SIGSEGV.

CWE:
CWE-476 - NULL Pointer Dereference

Affected Component

...
media_tools/isom_tools.c:979
Function:
gf_media_get_color_info()
...

Affected Product:
MP4Box (GPAC Multimedia Open Source

Affected
Version:
2.5-DEV-
rev1780-
g50b5741f
2-master;
commit
`50b5741f2
91126b610
c59db433f
c02e8a17f
0c5d`. Any
codebase
equivalent
to this
commit
that has
not applied
the fix
commit is
affected.

Attack
Conditions:
An attacker
supplies a
specially
crafted
MP4 file
containing
a video
sample
entry
whose type
(e.g.,
`v210`)
holds an
incompatib
le child box

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

Local access is required; the victim must process the file with `MP4Box -split-size 8000 <crafted\_file>` or any equivalent MP4Box operation that triggers muxer PID setup.

Impact:
The NULL pointer dereference (READ at address 0x8) causes an immediate process crash, resulting in Denial of Service. No evidence of arbitrary code execution was

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

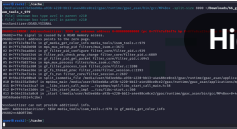
access is a near-NULL read that is not exploitable for control-flow hijacking.

Fix / mitigation status:
The fix adds the missing NULL check in ``gf_media_get_color_info`` before dereferencing the color-info pointer. Users should upgrade to the release containing commit ``9beed3c0a2f38505c745e5376234e7ed66e8e0b1`` or apply that patch directly.

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

- PoC:
[github.com/sigdevel/pocs/blob/...](#)
- Issue:
[github.com/gpac/gpac/issues/333...](#)
- Fix:
[github.com/gpac/gpac/commit/9b...](#)

Credit
[@sigdevel](#)



- #fuzzing
- #infosec
- #security

...and 9 more

May
29,
2026, · 🌐 · We
05:32
PM

0 boosts · 0 qu

