
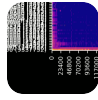


[Skip to main content](#) 1

[Skip to main navigation](#) 2

← Post 



sigd...
@si...

Security
Advisory:
CVE-2025-
60481 -
Out-of-
Bounds
Read in
GPAC/MP4
Box

Processing
a crafted
AC-4
stream
with an
invalid
`frame_rate
_index`
triggers an
out-of-
bounds
read in
`gf_odf_ac
4_cfg_dsi_v
1`, causing
MP4Box to
crash.

Summary:
The
`gf_odf_ac
4_cfg_dsi_v

Create account

Login



```
`odf/descri  
ptors.c`  
uses a  
stream-  
supplied  
`frame_rate  
_index` to  
index into  
fixed-size  
lookup  
tables  
(`AC4_SAM  
PLE_DELTA  
_TABLE_48  
`,  
`AC4_MEDI  
A_TIMESC  
ALE_48`)  
The  
function  
does not  
validate  
that the  
index is  
within  
bounds  
before  
performing  
the table  
lookup. A  
crafted AC-  
4 file  
carrying an  
out-of-  
range index  
(e.g., 15)  
causes an  
out-of-  
bounds
```

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

ultimately resulting in a NULL dereference and process crash.

CWE:
CWE-125 - Out-of-bounds Read

Affected Component:

...

odf/descriptors.c:2179

Function:
gf_odf_ac4_cfg_dsi_v1()
...

Affected Product:
MP4Box (GPAC Multimedia Open Source Project)

Affected Version:
2.5 DEV

Create account

Login

g856674b2
2-master;
commit
`856674b2
26d6cbe28
a941ad223
be38194cb
f7d37`. Any
codebase
equivalent
to this
commit
that has
not applied
the fix
commit is
affected.

Attack
Conditions:
An attacker
supplies a
specially
crafted AC-
4 stream
file
containing
an invalid
`frame_rate`
_index`
value.
Local
access is
required;
the victim
must
invoke
`MP4Box -
dash 100`

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

equivalent
DASH
segmentati
on
command
that
triggers the
AC-4
configurati
on
descriptor
parsing
path.

Impact:
The out-of-
bounds
read leads
to an
immediate
process
crash
(SEGV
READ at
address
0x0000000
00000),
resulting in
Denial of
Service. No
evidence of
arbitrary
code
execution
was
observed.

Fix /
mitigation

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

adds
bounds
validation
for
`frame_rate`
_index`
before the
fixed-size
table
lookups in
`gf_odf_ac`
4_cfg_dsi_v`
1`. Users
should
upgrade to
the release
containing
commit
`13eb5b76`
560aaf781`
3b865a2ad`
433258478`
e2695` or
apply that
patch
directly.


References

- Issue:
github.com/gpac/gpac/issues/3333
- PoC:
github.com/sigdevel/pocs/blob/...
- Fix:

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

[c/commit/13...](#)

Credit
[@sigdevel](#)



[#fuzzing](#)

[#infosec](#)

[#security](#)

...and 9 more

May 29, 2026, · 🌐 · We

05:58 PM

0 boosts · 0 qu

↩️ ↻ ⭐ 📌 ...

Create account

Login