



sigd...
@si...

Security
Advisory:
CVE-2025-
55641 -
NULL
Pointer
Dereferenc
e in GPAC
MP4Box
Sample
Info Copy

Processing
a crafted
MP4 file
with
corrupted
Sample
Auxiliary
Informatio
n metadata
can trigger
a NULL
pointer
dereferenc
e in
`gf_isom_c
opy_sampl
e_info()`,
causing a
Denial of
Service and
potential

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

corruption
impact.

Summary:

The
`gf_isom_c
opy_sampl
e_info()`
function in
`isomedia/i
som_write.
c` does not
sufficiently
validate
pointers
after
handling
invalid
Sample
Auxiliary
Informatio
n (SAI)
metadata.
A crafted
MP4 file
can provide
corrupted
SAI values,
such as an
invalid
`sai_sampl
es` count,
causing
memory
allocation
or merge
handling to
fail. The
import

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

copy
sample
informatio
n from a
NULL
pointer.

AddressSa
nitizer
reports a
`SEGV`
caused by
a `READ`
memory
access at
address
`0x000000
000000`,
with the
crash
occurring
at
`isomedia/i
som_write.
c:8164`.

CWE:
CWE-476 -
NULL
Pointer
Dereferenc
e

Affected
Componen
t:
...

isomedia/i
som_write.

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

```
gf_isom_co  
py_sample  
_info()  
'''
```

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
MP4Box
versions
2.4 and
earlier are
affected
according
to the
prepared
CVE/MITR
E data. The
issue was
reproduced
on a GPAC
build at
commit:
'''

```
f87b30611  
380e4dcd0  
3cd4dd9ac  
553c0ec33  
6826  
'''
```

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

An attacker supplies a crafted MP4 file containing corrupted SAI metadata. The issue can be reproduced locally with:

```
...  
./MP4Box -  
add  
13_poc.mp  
4 -new  
/dev/null -  
split-size  
500  
...
```

No elevated privileges are required. User interaction is required when the victim manually processes the malicious MP4 file, or an automated

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

workflow
invokes
MP4Box on
attacker-
controlled
input.

Impact:
The
immediate
observed
impact is
Denial of
Service due
to process
termination
. The local
CVE/MITR
E data also
marks
potential
code
execution
impact; the
observed
ASAN trace
is a NULL
pointer
read.

Fix /
mitigation
status:
The issue
was fixed
in GPAC
commit:
``
e38d24b7e

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

90ac3f208

0b52

...

Users should update to a GPAC build containing this commit or later. The affected code should validate SAI metadata, allocation results, and sample-info pointers before copying sample information.

References

:

- Issue:

[github.com/gpac/gpac/issues/31...](https://github.com/gpac/gpac/issues/31)

- PoC:

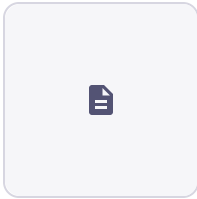
github.com/sigdevel/pocs/blob/...

Create account

Login

/gpac/gpac/commit/e3...

Credit:
@sigdevel
(Alexander A. Shvedov)



- #fuzzing
- #infosec
- #security

...and 11 more

Jun 12, 2026, 10:57 AM

Last edited Jun 12, 11:23 AM

0 boosts · 0 quotes





EN

@sigdevel

Hello

, please

e

add

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!

↩ 0