

[Skip to main content](#) 1

[Skip to main navigation](#) 2

← Post 



sigd...
@si...

Security
Advisory:
CVE-2025-
55659 -
NULL
Pointer
Dereferenc
e in GPAC
MP4Box
`ctts_box_
write`

Processing
a crafted or
truncated
MP4 file
with
`MP4Box`
can trigger
a NULL
pointer
dereferenc
e in
`ctts_box_
write()`,
causing a
Denial of
Service.

Summary:
The
`ctts_box_

Create account

Login



`isomedia/
box_code_
base.c`
does not
sufficiently
validate
critical
pointers
and
timestamp-
derived
state when
writing the
compositio
n time-to-
sample
(`ctts`) box.
When
MP4Box
processes
a crafted
truncated
MP4 file
during
split/remux
operations,
negative
timestamp
handling
can leave
the
compositio
n-time
entries
pointer in
an invalid
or NULL
state. The
write path

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

dereferenc
es the
NULL
pointer and
crashes.

AddressSa
nitizer
reports a
`SEGV`
caused by
a `READ`
memory
access at
address
`0x000000
000000`,
with the
crash
occurring
at
`isomedia/
box_code_
base.c:464`
`.

CWE:
CWE-476 -
NULL
Pointer
Dereferenc
e

Affected
Componen
t:
`...`

isomedia/b
ox_code_b

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

```
ctts_box_w  
rite()  
...  

```

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:

```
...  
ff8249a40  
7685d00ce  
b5f4d2a79  
8b9cad195  
140e  
...  

```

Create account

Login

fix commit
`2476b140
58761845a
d6ccee43d
cf5d49ca9
cca95`
should be
considered
affected if
they
contain the
vulnerable
`ctts_box_
write()`
path.

Attack
Conditions:
An attacker
supplies a
crafted or
truncated
MP4 file
with
timestamp
data that
causes
invalid
negative
timestamp
handling
during
split/remux
processing
. The issue
can be
reproduced
locally
with:

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

```
```
```

```
./MP4Box -
add
5_poc.mp4
-new ./test
-split-size
500
```
```

No elevated privileges are required. User interaction is required when the victim manually processes the malicious MP4 file, or an automated workflow invokes MP4Box on attacker-controlled media.

Impact:
The immediate observed impact is Denial of

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

termination
. The crash
is a NULL
pointer
dereferenc
e on the
zero page;
no
evidence of
arbitrary
code
execution
was
observed.

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

...

2476b1405
8761845ad
6ccee43dc
f5d49ca9c
ca95

...

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

Create account

Login

should validate composition-time entries and timestamp-derived state before writing the `ctts` box, and malformed/truncated MP4 inputs should be rejected cleanly.

References
:

- Issue:
github.com/gpac/gpac/issues/31...

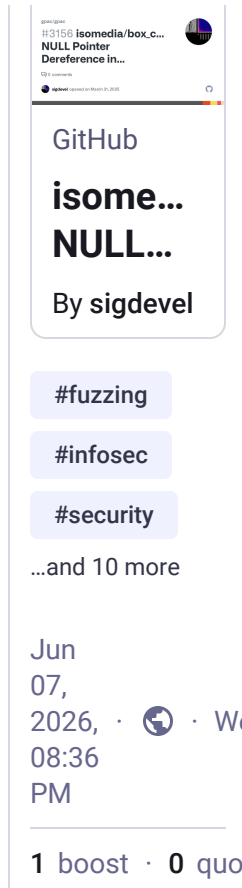
- PoC:
github.com/sigdevel/pocs/blob/...

- Fix:
github.com/gpac/gpac/commit/24...

Credit
[@sigdevel](https://github.com/sigdevel)

Create account

Login



The screenshot shows a GitHub repository page. At the top, it displays the repository name "#3156 isome... NULL Pointer Dereference in...". Below the repository name, it says "By sigdevel". There are three tags: "#fuzzing", "#infosec", and "#security", followed by "...and 10 more". The date and time are "Jun 07, 2026, 08:36 PM". At the bottom, it shows "1 boost · 0 quor".

Create account

Login