

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
55639 -
NULL
Pointer
Dereferenc
e in GPAC
MP4Box
Track Kind
Handling

Processing
a crafted
MP4 file
with
MP4Box ` -
add` can
trigger a
NULL
pointer
dereferenc
e in
`gf_isom_a
dd_track_ki
nd()`,
causing a
Denial of
Service.

Summary:
The
`gf_isom_a
dd_track_ki

Create account

Login



function in
`isomedia/i
som_write.
c` does not
sufficiently
validate the
`kind`
string
before
passing it
to
`strdup()`.
When
MP4Box
imports a
specially
crafted
MP4 file
containing
corrupted
MPEG-2 TS
PMT
descriptors
and empty
track
metadata,
a NULL
`kind`
pointer can
reach
`gf_isom_a
dd_track_ki
nd()`.

AddressSa
nitizer
reports a
segmentati
on fault

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

```
address
`0x0` in
`strlen()`
during
`strdup()`,
reached
from
`gf_isom_a
dd_track_ki
nd()` at
`isomedia/i
som_write.
c:3153`.
```

CWE:
CWE-476 -
NULL
Pointer
Dereferenc
e

Affected
Componen
t:
...

```
isomedia/i
som_write.
c:3153
Function:
gf_isom_ad
d_track_kin
d()
..
```

Affected
Product:
MP4Box
(GPAC
Multimedia

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

Source
Project)

Affected
Version:
MP4Box
version 2.4
is affected
according
to the
prepared
CVE/MITR
E data. The
issue was
reproduced
on a GPAC
build at
commit:
...

78c2c9be2
9a41b38ec
a2c53d280
442088a71
dab9
...

Builds
before the
fix commit
`027ce139
dda498ee9
5df36db9f
9f6f3cadce
8ec9`
should be
considered
affected if
they
contain the
vulnerable

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

handling
path.

Attack
Conditions:
An attacker
supplies a
crafted
MP4 file
with
corrupted
PMT
descriptors
in an
MPEG-2 TS
stream and
malformed
or empty
track
metadata.
The issue
can be
reproduced
locally
with:

```
...  
./MP4Box -  
add  
23_poc.mp  
4 -new  
/dev/null  
...
```

No
elevated
privileges
are
required.

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

is required when the victim manually processes the malicious file, or an automated media workflow invokes MP4Box on attacker-controlled input.

Impact:
The immediate observed impact is Denial of Service due to process termination . No evidence of arbitrary code execution was observed.

Fix / mitigation status:
The issue was fixed

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

```\n

```
027ce139d
da498ee95
df36db9f9f
6f3cadce8
ec9
```

```\n

Users should update to a GPAC build containing this commit or later. The affected track metadata path should validate `kind` before duplicating it and fail cleanly when malformed input omits the expected metadata.

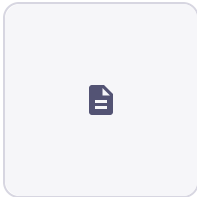
References
:

- Issue:
github.com

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

2...
- PoC:
[github.com/sigdevel/pocs/blob/...](#)
- Fix:
[github.com/gpac/gpac/commit/02...](#)
- CVE record:
[cve.org/CVERecord?id=CVE-2025-...](#)

Credit
Alexander
A. Shvedov
([@sigdevel](#))



- #fuzzing
- #infosec
- #security

...and 11 more

Jun
18,
2026, · 🌐 · We
04:19
AM

0 boosts · 0 qu

Create account

Login

—

|

|

Create account

Login