

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
55657 -
NULL
Pointer
Dereferenc
e in GPAC
MP4Box
VVC
Configurati
on Writer

Processing
a crafted
MP4 file
containing
malformed
or
unsupporte
d VVC
configurati
on data
with
`MP4Box`
can trigger
a NULL
pointer
dereferenc
e in
`gf_odf_vvc
_cfg_write_
bs()`,

Create account

Login



Denial of Service.

Summary:

The ``gf_odf_vvc`_cfg_write_bs()` function in ``odf/descriptors.c`` does not validate that the pointer to VVC configuration on NAL unit data is non-NULL before using it. When MP4Box processes a crafted MP4 file containing an unsupported ``vvc16`` box inside the ``std`` parent box, the VVC configuration write path can receive a

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

on pointer
and
dereferenc
e it.

AddressSa
nitizer
reports a
`SEGV`
caused by
a `READ`
memory
access at
address
`0x000000
000000`,
with the
crash
occurring
at
`odf/descri
ptors.c:126
7`.

CWE:
CWE-476 -
NULL
Pointer
Dereferenc
e

Affected
Componen
t:
...

odf/descri
ptors.c:126
7
Function:

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

bs()
...

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
...

Builds

Create account

Login

`34495b9d
b132be2ad
b6edd2ab7
a28e5f8d5
cd2e5`
should be
considered
affected if
they
contain the
vulnerable
VVC
configurati
on write
path.

Attack
Conditions:
An attacker
supplies a
crafted
MP4 file
containing
malformed
VVC
configurati
on data,
including
an
unsupporte
d `vvc16`
sample
description
box. The
issue can
be
reproduced
locally
with:

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

```
'''
```

```
./MP4Box -  
add  
6_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:

...

34495b9db
132be2adb
6edd2ab7a
28e5f8d5c
d2e5

...

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

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

should
validate
VVC
configurati
on pointers
and reject
malformed
or
unsupporte
d VVC
sample
description
data before
writing
VVC
configurati
on records.

References :

- Issue:
[github.com
/gpac/gpa
c/issues/3
1...](https://github.com/gpac/gpac/issues/31)

- PoC:
[github.com
/sigdevel/p
ocs/blob/...](https://github.com/sigdevel/pocs/blob/...)

- Fix:
[github.com
/gpac/gpa
c/commit/
34...](https://github.com/gpac/gpac/commit/34...)

Credit
[@sigdevel](#)

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

#fuzzing

#infosec

#security

...and 11 more

Jun 07, 2026, ·  · We

08:39 PM

Last edited

Jun 12, 11:25 AM

0 boosts · 0 qu

