

[← P...](#) 

sigd...
@si...

Security
Advisory:
CVE-2025-
60464 -
Use-After-
Free in
GPAC
MP4Box
SEI State
Handling

Processing
a crafted
MPEG-2 TS
file with
MP4Box ` -
info` can
trigger a
heap use-
after-free in
`gf_sei_loa
d_from_sta
te_internal(
)`), causing
a crash and
potential
code
execution.

Summary:
The
`gf_sei_loa
d_from_sta
te_internal/

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

in
`filters/sei_
load.c` can
access
codec/SEI
state after
the related
heap buffer
has been
freed by
the NALU
demuxer
setup path.
When
MP4Box
processes
a specially
crafted
MPEG-2
Transport
Stream file
containing
malformed
AVC/HEVC
/VVC NAL
units and
corrupted
PMT
descriptors
,
`naludmx_c
onfigure_pi
d()` can
release a
state buffer
that is later
read during
SEI state
loading

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

CWE:
CWE-416 -
Use After
Free

Affected
Component:
...

filters/sei_load.c:225
Function:
gf_sei_load
_from_state_internal()
...

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected
Version:
The issue
was
reproduced
on:
...

GPAC
version:
2.5-DEV-
rev1557-
g62714f27
c-master

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

64a3d1eb7
e880f9eed
2d38673cb
43ce
...

The MITRE
response
states that
GPAC
Project/MP
4Box
before
`26.02.0` is
affected.
Builds
before the
fix commit
`8f404bd58
1e4552674
82f862721
69a742f65
4b97`
should be
considered
affected if
they
contain the
vulnerable
SEI state
handling
path.

Attack
Conditions:
An attacker
supplies a
crafted
MPEG-2 TS

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

malformed
AVC/HEVC
/VVC
bitstream
data,
corrupted
PMT
descriptors
, and
invalid
NAL/SEI
state. The
issue can
be
reproduced
locally
with:

```
...  
  
./MP4Box -  
info  
32_filters_s  
ei_load_c_2  
25_in_gf_s  
ei_load_fro  
m_state_int  
ernal  
...
```

No
elevated
privileges
are
required.
User
interaction
is required
when the
victim
manually

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

malicious
file, or an
automated
media
workflow
invokes
MP4Box on
attacker-
controlled
input.

The
prepared
CVSS
vector in
the local
BDU data
is:

...

AV:L/AC:L/
PR:N/UI:R/
S:U/C:H/I:H
/A:H

...

Impact:
The
immediate
observed
impact is
Denial of
Service due
to process
termination
. Because
the
vulnerabilit
y is a heap

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

memory
corruption
and
potential
arbitrary
code
execution
are
possible.

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

...

8f404bd58
1e4552674
82f862721
69a742f65
4b97

...

Users
should
update to a
GPAC build
containing
this
commit or
later. The
affected
SEI/NALU
handling
path
should
ensure

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

remain
valid
before SEI
parsing
reads from
them.

References :

- Issue:

[github.com
/gpac/gpa
c/issues/3
2...](https://github.com/gpac/gpac/issues/32...)

- PoC:

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

- Fix:

[github.com
/gpac/gpa
c/commit/
8f...](https://github.com/gpac/gpac/commit/8f...)

- CVE
record:
[cve.org/CV
ERecord?
id=CVE-
2025-...](https://cve.org/CVERecord?id=CVE-2025-...)

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



Create account

Login

#fuzzing

#infosec

#security

...and 11 more

Jun 19, 2026, · 🌐 · We

07:15 PM

0 boosts · 0 qu

⏮️ ↺️ ⭐️ 📌 ...