

← P... 🔒



sigd...
@si...

Security
Advisory:
CVE-2025-
55649 -
NULL
Pointer
Dereferenc
e in GPAC
MP4Box
ESD
Mapping

Processing
a crafted
MP4 file
with
corrupted
Elementary
Stream
Descriptor
data can
trigger a
NULL
pointer
dereferenc
e in
`gf_media_
map_esd()`
, causing a
Denial of
Service.

Summary:
The

Create account

Login



map_esd() function in media_tools/isom_tools.c does not verify that esd->URLString is non-NULL before passing it to strlen(). When MP4Box processes a crafted MP4 file containing corrupted ESD data during fragmentation setup, URLString can be NULL and the process crashes while reading from address 0x000000000000.

AddressSa

Create account

Login

`SEGV` in
`strlen()`,
with the
GPAC call
site at
`media\_tools/isom\_tools.c:1359`
.

CWE:
CWE-476 -
NULL
Pointer
Dereference

Affected
Component:
...

media_tools/isom_tools.c:1359
Function:
gf_media_map_esd()
...

Affected
Product:
MP4Box
(GPAC
Multimedia
Open
Source
Project)

Affected

Create account

Login

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:

...

09e7063ed
0a13b4cee
9a180a56d
cc21e9f9a
de07

...

Attack
Conditions:
An attacker
supplies a
crafted
MP4 file
containing
corrupted
ESD data.
The issue
can be
reproduced
locally
with:

...

./MP4Box -
frac 1500

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

``

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 Service due to process termination . The crash is a NULL pointer dereference on the

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

evidence of
arbitrary
code
execution
was
observed.

Fix /
mitigation
status:

The local
CVE/MITR
E data
references
GPAC fix
commit:
...

10c16d546
59b1b82dd
49573dfea
cfa9a5627
a115
...

Users
should
update to a
GPAC build
containing
this
commit or
later. The
affected
code
should
validate
`esd`, `esd-
>URLString
, and
related ESD

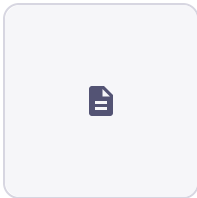
[Create account](#)[Login](#)

string
operations.

References
:

- Issue:
[github.com/gpac/gpac/issues/31...](#)
- PoC:
[github.com/sigdevel/pocs/blob/...](#)
- Fix:
[github.com/gpac/gpac/commit/10...](#)

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



- #fuzzing
- #infosec
- #security

...and 11 more

Jun
12,
2026, · · We
10:45

Last edited
Jun 12, 11:23
AM

0 boosts · 0 quotes

← ↻ ☆ 📌 ...

 EN 🗨️ 🌐

@sigdevel

Hello,

please add direct references to the CVE too. Right now there is only this Mastodon toot. Please add direct references also to the

Create account

Login

https://infosec.exchange/@sigdevel/116736730620435563

8/9

"PoC
" and
"Fix"
you
have
shar
ed in
this
too.

Than
ks!

↩ 0