Skip to main content 1
Skip to main navigation 2

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_load_from_state_internal()`, causing a crash and potential code execution.

Summary: The `gf_sei_loa

)` function 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_configure_pid()` can release a state buffer that is later read during SEI state

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-g62714f27c-master
```

64a3d1eb7e880f9eed2d38673cb43ce
```

The MITRE response states that GPAC Project/MP4Box before `26.02.0` is affected. Builds before the fix commit `8f404bd581e455267482f86272169a742f654b97` should be considered affected if they contain the vulnerable SEI state handling path.

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

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_sei_load_c_225_in_gf_sei_load_from_state_internal
```

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

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 vulnerability is a heap

memory corruption and potential arbitrary code execution are possible.

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

```
8f404bd581e455267482f86272169a742f654b97
```

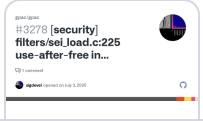
Users should update to a GPAC build containing this commit or later. The affected SEI/NALU handling path should ensure

remain valid before SEI parsing reads from them.

References:

- Issue: github.com/gpac/gpac/issues/32...
- PoC: github.com/sigdevel/pocs/blob/...
- Fix: github.com/gpac/gpac/commit/8f...
- CVE record: cve.org/CVERecord?id=CVE-2025-...

Credit Alexander A. Shvedov (@sigdevel)



[securi… filters/…

By **sigdevel**

#fuzzing

#infosec

#security

…and 11 more

Jun 19, 2026, · · We 07:15 PM

0 boosts · **0** qu