Skip to main content 1
Skip to main navigation 2

Pos

sigd...
@si...

Security Advisory: CVE-2025-52293 - Memory Safety Violation in GPAC MP4Box HEVC SPS Parser

Processing a crafted MP4 file containing malformed HEVC SPS data with `MP4Box` can trigger a segmentation fault in `gf_hevc_read_sps_bs_internal()`, causing a Denial of Service.

Summary:

ad_sps_bs_internal()` function in `media_tools/av_parsers.c` does not safely handle crafted HEVC SPS data while parsing video configuration from a malicious MP4 file. During import and split processing, malformed SPS data reaches the HEVC parser and causes an invalid memory read.

AddressSanitizer reports a `SEGV` caused by a `READ` memory access at

rs.c:9309`. The crash occurs while MP4Box processes the crafted file through the isomedia input and NAL replacement/configuration path.

CWE: CWE classification was not specified in the local MITRE data. This issue is best described as a memory safety violation in HEVC SPS parsing, with an observed out-of-bounds/invalid read leading to

Affected Component:
```
media_tools/av_parsers.c:9309
Function: gf_hevc_read_sps_bs_internal()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version: MP4Box versions 2.4 and earlier (GPAC build at commit: 8a0d5b43c242fe4befb88530e4c9afef37114161)

Attack Conditions:

crafted MP4 file containing malformed HEVC SPS NAL units. The issue can be reproduced locally with:

```
./MP4Box -add 3_poc.mp4 -new /dev/null -split-size 5000000
```

No elevated privileges are required. User interaction is required when the victim manually processes the malicious MP4 file, or an automated workflow

attacker-controlled media.

Impact: The immediate observed impact is Denial of Service due to process termination. The local CVE request classifies the issue as a buffer overflow / memory safety violation. The observed ASAN trace shows an invalid read; no evidence of arbitrary code execution was observed.

Fix / mitigation status:

in GPAC commit:

```
d091c7e92ef0b6497b808e243501f500135f69c4
```

Users should update to a GPAC build containing this commit or later. The parser should validate HEVC SPS bitstream boundaries and reject malformed SPS/NAL data before reading fields from the bitstream.

References:

- Issue: github.com

1…
- PoC: github.com/sigdevel/pocs/blob/…
- Fix: github.com/gpac/gpac/commit/d0…

Credit @sigdevel

#fuzzing
#infosec
#security
…and 10 more

Jun 07, 2026, 07:30 PM · · We

2 boosts · 0 qu