

sigd...
@si...

Security Advisory: CVE-2025-70116 - NULL Pointer Dereference in GPAC MP4Box

A NULL pointer dereference vulnerability was identified in GPAC MP4Box when processing certain malformed or truncated MP4 files.

Summary: When MP4Box parses a specially crafted damaged

Create account Login

an invalid or incomplete stsd entry may result in missing descriptor data. In the affected code path, gf_media_map_esd() in src/media_tools/isom_tools.c may dereference a NULL pointer, leading to a crash.

Affected component: src/media_tools/isom_tools.c Function: gf_media_map_esd()

Affected product: GPAC MP4Box

Affected

Create account Login

was reproduced on GPAC version 2.5-DEV-rev1815-g261ffdd13-master / MP4Box commit 261ffdd135eee8f646eb9326a43438b32a7ad3a1.

Attack conditions: Exploitation requires local access or another way to make the vulnerable MP4Box instance process a malformed or truncated MP4 file. The issue is triggered during local processing of the

Create account Login

Impact: Successful exploitation causes a segmentation fault and terminates the MP4Box process, resulting in a local denial of service (DoS). No evidence of code execution has been identified.

CWE: CWE-476 - NULL Pointer Dereference

Fixed version: The issue has been fixed in GPAC commit 56d21ea812fd5ba83e6c0177727

Create account Login

are advised to update to a GPAC build that includes this commit or apply the patch manually.

References:
Issue: github.com/gpac/gpac/issues/33…
PoC: github.com/sigdevel/pocs/blob/…
Fix: github.com/gpac/gpac/commit/56…

Credits: @sigdevel

cve.org/CVERecord?id=CVE-2025-…



Create account Login

#security

...and 9 more

May 23, 2026, 03:20 PM · · We

Last edited **May 27, 07:25 PM**

0 boosts · **0** qu

Create account Login