Skip to main content 1
Skip to main navigation 2

Pos

sigd...
@si...

Security Advisory: CVE-2025-52292 - Stack-based Buffer Overflow in GPAC/MP4 Box

Processing a crafted MP4 file with `MP4Box` can trigger a stack-based buffer overflow in `filein_process()` in `filters/in_file.c`, causing a crash and potential memory corruption.

Summary:

ess()` function formats a status string into a fixed-size stack buffer using an unsafe `sprintf()` call. When the source path or basename derived from `ctx->src` is long or specially crafted, the generated status string can exceed the 1024-byte `szStatus` stack buffer. AddressSanitizer reports a `stack-buffer-overflow` at `filters/in_file.c:700`, with a

size 1811` overflowing the `szStatus` object allocated in the `filein_process()` stack frame. The crash is reachable while MP4Box processes a crafted MP4 file through DASH/file-list handling.

CWE: CWE-121 - Stack-based Buffer Overflow

Affected Component:
```
filters/in_file.c:700
Function: filein_process()
```

Affected Product: MP4Box (GPAC Multimedia Open Source Project)

Affected Version: 2.5-DEV-rev1174-g3017379f1-master

Attack Conditions: An attacker supplies a crafted MP4 file or causes MP4Box to process a crafted input path/name that expands into an oversized status string. The issue can be reproduced locally with:

dash 1000 /dev/null 1_poc.mp4
```

No elevated privileges are required. User interaction is required when the victim manually processes the malicious file with MP4Box or an automated workflow invokes MP4Box on attacker-controlled media.

Impact: The immediate observed impact is Denial of Service due to process termination. Because
```

y is a stack-based buffer overflow with an attacker-influenced write, memory corruption and potential arbitrary code execution cannot be ruled out.

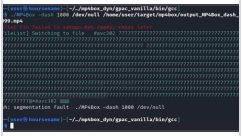
Fix / mitigation status:
The issue was fixed in GPAC commit:
```
bc2fd5bb5c31ae148624767c4a7a17f02c42951b
```
Users should update to a GPAC build containing this

vulnerable status-string formatting path should use bounded formatting with the destination buffer size and should ensure that formatted status messages are truncated or rejected safely.

References:

- Issue: github.com/gpac/gpac/issues/31…
- PoC: github.com/sigdevel/pocs/blob/…
- Fix: github.com/gpac/gpac/commit/bc…

A. Shvedov (@sigdevel)



#fuzzing

#infosec

#security

...and 10 more

Jun 07, 2026, · · We 05:54 AM

Last edited **Jun 07, 05:55 AM**

0 boosts · **0** qu