



index : mupdf.git

MuPDF library

master

Chris Liddell

summary refs log tree **commit** diff

log msg

author Tor Andersson <tor.andersson@artifex.com> 2026-01-05 17:54:15 +0100
 committer Tor Andersson <tor.andersson@artifex.com> 2026-01-05 18:12:02 +0100
 commit [a26f0142e7d390d4a82c6e5ae0e312e07cc4ec85](#) (patch)
 tree [29c0d1367b379c4cb398158691573288a5a3bc57](#)
 parent [fc8ff4e1b62f001717b339a81c1753ad30374bea](#) (diff)

diff options

context:
 space:
 mode:

Bug 708990: Avoid overflow src_stride calculation in unpack_stream.

By using 64-bit math!

Diffstat

```
-rw-r--r-- source/fitz/draw-unpack.c 2
```

1 files changed, 1 insertions, 1 deletions

```
diff --git a/source/fitz/draw-unpack.c b/source/fitz/draw-unpack.c
index 048abbf35..8c99337db 100644
--- a/source/fitz/draw-unpack.c
+++ b/source/fitz/draw-unpack.c
@@ -437,7 +437,7 @@ unpack_drop(fz_context *ctx, void *state)
 fz_stream *
 fz_unpack_stream(fz_context *ctx, fz_stream *src, int depth, int w, int h, int n, int indexed, int pad, int skip)
 {
-   int src_stride = (w*depth*n+7)>>3;
+   int src_stride = ((int64_t)w*depth*n+7)>>3; // avoid overflow by bumping to 64-bit math
   int dst_stride;
   unpack_state *state;
   fz_unpack_line_fn unpack_line = NULL;
```

generated by cgkit v1.2.3 (git 2.25.1) at 2026-04-21 10:13:06 +0000