ArtifexSoftware / **mupdf** Public

Code | Pull requests 53 | Actions | Projects | Security and quality | Insights

Commit a26f014

artifex-tor committed on Jan 5

```
Bug 708990: Avoid overflow src_stride calculation in unpack_stream.

By using 64-bit math!
```

master

1 parent fc8ff4e commit a26f014

1 file changed +1 -1 lines changed

Top

Filter files…

source/fitz

draw-unpack.c

1 file changed +1 -1 lines changed

Search within code

source/fitz/draw-unpack.c

```
@@ -437,7 +437,7 @@ unpack_drop(fz_context *ctx, void *state)
437 437  fz_stream *
438 438  fz_unpack_stream(fz_context *ctx, fz_stream *src, int depth, int w, int h, int
         n, int indexed, int pad, int skip)
439 439  {
440     -     int src_stride = (w*depth*n+7)>>3;
    440  +     int src_stride = ((int64_t)w*depth*n+7)>>3; // avoid overflow by bumping to
         64-bit math
441 441      int dst_stride;
442 442      unpack_state *state;
443 443      fz_unpack_line_fn unpack_line = NULL;
```

Comments 0

Please sign in to comment.