Bug 703076 - Buffer Overflow in tiff_expand_colormap() function in source/fitz/load-tiff.c:256:25

Status: RESOLVED FIXED

Alias: None

Product: MuPDF
Component: mupdf (show other bugs)
Version: 1.18.0
Hardware: PC Linux

Importance: P4 normal
Assignee: muPDF bugs

URL:
Keywords:

Duplicates (1): ~~703075~~ (view as bug list)
Depends on:
Blocks:

Reported: 2020-10-30 12:35 UTC by cylin
Modified: 2021-09-15 14:21 UTC (History)
CC List: 3 users (show)

See Also:
Customer:
Word Size: ---

Attachments	
A tiff file whose samplesperpixel == 1 and extrasamples == 4 (460 bytes, image/tiff) 2020-10-30 12:35 UTC, cylin	Details
Add an attachment (proposed patch, testcase, etc.)	

Note
You need to log in before you can comment on or make changes to this bug.

cylin 2020-10-30 12:35:30 UTC **Description**

Created attachment 20086 [details]
A tiff file whose samplesperpixel == 1 and extrasamples == 4

Hello,

There is a buffer overflow in tiff_expand_colormap() function in file source/fitz/load-tiff.c. In this function, a buffer is allocated from heap to store the colormap information:

```
> stride = tiff->imagewidth * (tiff->samplesperpixel + 2) * 2;
> samples = Memento_label(fz_malloc(ctx, (size_t)stride * tiff->imagelength), "tiff
```

But during the follow loop, if the extrasamples of tiff is not equal to 0, this can cause an overflow:

```
> for (y = 0; y < tiff->imagelength; y++)  // 32
> {
>     src = tiff->samples + (unsigned int)(tiff->stride * y);
>     dst = samples + (unsigned int)(stride * y);
>
>     for (x = 0; x < tiff->imagewidth; x++)
>     {
>         if (tiff->extrasamples)
>         {
>             int c = tiff_getcomp(src, x * 2, tiff->bitspersample);
>             int a = tiff_getcomp(src, x * 2 + 1, tiff->bitspersample);
>             *dst++ = tiff->colormap[c + 0] >> 8;
>             *dst++ = tiff->colormap[c + 0];
>             *dst++ = tiff->colormap[c + maxval] >> 8;
>             *dst++ = tiff->colormap[c + maxval];
>             *dst++ = tiff->colormap[c + maxval * 2] >> 8;
>             *dst++ = tiff->colormap[c + maxval * 2];
>             if (tiff->bitspersample <= 16)
>                 *dst++ = a << (16 - tiff->bitspersample);
>             else
>                 *dst++ = a >> (tiff->bitspersample - 16);
>         }
>         // ...
>     }
>     // ...
> }
```

Robin Watts 2021-02-26 16:13:45 UTC **Comment 1**

Fix in testing:

https://git.ghostscript.com/?p=user/robin/mupdf.git;a=commitdiff;h=8b0120cfd51b7f8db2409a4cdcc4d916df590160

Robin Watts 2021-02-26 16:20:53 UTC **Comment 2**

*** ~~Bug 703075~~ has been marked as a duplicate of this bug. ***