

This repository was archived by the owner on Dec 1, 2017. It is now read-only.

vadz / libtiff Public archive

Code Pull requests Actions Security Insights

# Commit 5c08029



erouault committed on Jan 11, 2017

```
* tools/tiffcp.c: error out cleanly in cpContig2SeparateByRow and
cpSeparate2ContigByRow if BitsPerSample != 8 to avoid heap based overflow.
Fixes http://bugzilla.maptools.org/show\_bug.cgi?id=2656 and
http://bugzilla.maptools.org/show\_bug.cgi?id=2657
```

master · Release-v4-0-9 Release-v4-0-8

1 parent [393881d](#) commit 5c08029

2 files changed +29 -2 lines changed

↑ Top ⚙

Filter files...

- ChangeLog
- tools
  - tiffcp.c

2 files changed +29 -2 lines changed

Search within code ⚙

```
ChangeLog
... @@ -1,3 +1,10 @@
1 + 2017-01-11 Even Rouault <even.rouault at spatialys.com>
2 +
3 + * tools/tiffcp.c: error out cleanly in cpContig2SeparateByRow and
4 + cpSeparate2ContigByRow if BitsPerSample != 8 to avoid heap based overflow.
5 + Fixes http://bugzilla.maptools.org/show\_bug.cgi?id=2656 and
6 + http://bugzilla.maptools.org/show\_bug.cgi?id=2657
7 +
```

```

1      8      2017-01-11 Even Rouault <even.rouault at spatialys.com>
2      9
3     10      * libtiff/tiffio.h, tif_unix.c, tif_win32.c, tif_vms.c: add _TIFFcalloc()

```



tools/tiffcp.c



```
@@ -591,7 +591,7 @@ static copyFunc pickCopyFunc(TIFF*, TIFF*, uint16,
uint16);
```

```

591    591    static int
592    592    tiffcp(TIFF* in, TIFF* out)
593    593    {
594    -      uint16 bitspersample, samplesperpixel = 1;
594    +      uint16 bitspersample = 1, samplesperpixel = 1;
595    595    uint16 input_compression, input_photometric = PHOTOMETRIC_MINISBLACK;
596    596    copyFunc cf;
597    597    uint32 width, length;

```



```
@@ -1067,6 +1067,16 @@ DECLAREcpFunc(cpContig2SeparateByRow)
```

```

1067   1067   register uint32 n;
1068   1068   uint32 row;
1069   1069   tsample_t s;
1070   +      uint16 bps = 0;
1071   +
1072   +      (void) TIFFGetField(in, TIFFTAG_BITSPERSAMPLE, &bps);
1073   +      if( bps != 8 )
1074   +      {
1075   +          TIFFError(TIFFFileName(in),
1076   +                  "Error, can only handle BitsPerSample=8 in %s",
1077   +                  "cpContig2SeparateByRow");
1078   +          return 0;
1079   +      }

```

```

1070   1080
1071   1081   inbuf = _TIFFmalloc(scanlinesizein);
1072   1082   outbuf = _TIFFmalloc(scanlinesizeout);

```



```
@@ -1120,6 +1130,16 @@ DECLAREcpFunc(cpSeparate2ContigByRow)
```

```

1120   1130   register uint32 n;
1121   1131   uint32 row;
1122   1132   tsample_t s;
1133   +      uint16 bps = 0;

```

```

1134 +
1135 +     (void) TIFFGetField(in, TIFFTAG_BITSPERSAMPLE, &bps);
1136 +     if( bps != 8 )
1137 +     {
1138 +         TIFFError(TIFFFileName(in),
1139 +             "Error, can only handle BitsPerSample=8 in %s",
1140 +             "cpSeparate2ContigByRow");
1141 +         return 0;
1142 +     }
1123 1143
1124 1144     inbuf = _TIFFmalloc(scanlinesizein);
1125 1145     outbuf = _TIFFmalloc(scanlinesizeout);
@@ -1784,7 +1804,7 @@ pickCopyFunc(TIFF* in, TIFF* out, uint16
bitspersample, uint16 samplesperpixel)
1784 1804     uint32 w, l, tw, tl;
1785 1805     int bychunk;
1786 1806
1787 -     (void) TIFFGetField(in, TIFFTAG_PLANARCONFIG, &shortv);
1807 +     (void) TIFFGetFieldDefaulted(in, TIFFTAG_PLANARCONFIG, &shortv);
1788 1808     if (shortv != config && bitspersample != 8 && samplesperpixel > 1) {
1789 1809         fprintf(stderr,
1790 1810             "%s: Cannot handle different planar configuration w/ bits/sample
!= 8\n",

```

## Comments 0



This repository has been archived.