**TIFF CHANGE INFORMATION**

**Current Version**: v3.9.5  
**Previous Version**: [v3.9.4](http://docs.google.com/v3.9.4.html)  
**Master FTP Site**:  [download.osgeo.org](ftp://download.osgeo.org/libtiff), directory pub/libtiff  
**Master HTTP Site**: <http://www.simplesystems.org/libtiff/>

This document describes the changes made to the software between the *previous* and *current* versions (see above). If you don't find something listed here, then it was not done in this timeframe, or it was not considered important enough to be mentioned. The following information is located here:

* [Major Changes](#tyjcwt)
* [Changes in the software configuration](#30j0zll)
* [Changes in libtiff](#1fob9te)
* [Changes in the tools](#3znysh7)
* [Changes in the contrib area](#2et92p0)

**MAJOR CHANGES:**

* None

**CHANGES IN THE SOFTWARE CONFIGURATION:**

* configure.ac: Should use AC\_CANONICAL\_HOST since host specifies the run-time target whereas target is used to specify the final output target if the package is a build tool (like a compiler), which libtiff is not. Resolves libtiff bug 2307 "Use AC\_CANONICAL\_HOST macro".

**CHANGES IN LIBTIFF:**

* libtiff/tif\_getimage.c: Check the number of samples per pixel when working with YCbCr image in PickContigCase(). As per bug http://bugzilla.maptools.org/show\_bug.cgi?id=2216
* libtiff/tif\_dir.c: Set the bogus post-decoding hook when processing TIFFTAG\_BITSPERSAMPLE in \_TIFFVSetField() for the case of 8 bit when we don't need any post-processing. That helps to reset the hook if we previously set this field to some other value and the hook was initialized accordingly. As per bug http://bugzilla.maptools.org/show\_bug.cgi?id=2035
* libtiff/tif\_getimage.c: Avoid wrong math du to the signed/unsigned integer type conversions. As per bug http://bugzilla.maptools.org/show\_bug.cgi?id=2207
* libtiff/tif\_dirinfo.c: Don't use assertions in \_TIFFFieldWithTag() and \_TIFFFieldWithName() if the tag is not found in the tag table. This should be normal situation and returned NULL value should be properly handled by the caller.
* libtiff/{tif\_dirwrite.c, tif\_print.c}: Properly handle "DotRange" tag as it can be either byte or short size and should be set and read by value, not as an array. As per bug http://bugzilla.maptools.org/show\_bug.cgi?id=2116
* libtiff/tif\_dirread.c: Really reset the tag count in CheckDirCount() to expected value as the warning message suggests. As per bug http://bugzilla.maptools.org/show\_bug.cgi?id=1963
* libtiff/tif\_open.c: Fix mode check before opening a file. http://bugzilla.maptools.org/show\_bug.cgi?id=1906
* libtiff/tif\_jpeg.c, libtiff/tif\_strip.c: apply patch for CVE-2010-3087 per bug http://bugzilla.maptools.org/show\_bug.cgi?id=2140
* libtiff/tif\_dirread.c: fix crash when reading a badly-constructed TIFF per http://bugzilla.maptools.org/show\_bug.cgi?id=1994
* libtiff/tif\_ojpeg.c: fix buffer overflow on problem data http://bugzilla.maptools.org/show\_bug.cgi?id=1999
* libtiff/tif\_dirread.c: modify warnings http://bugzilla.maptools.org/show\_bug.cgi?id=2016
* libtiff/tif\_jpeg.c: fix use of clumplines calculation http://bugzilla.maptools.org/show\_bug.cgi?id=2149
* libtiff/tif\_color.c: prevent crash in handling bad TIFFs resolves CVE-2010-2595 http://bugzilla.maptools.org/show\_bug.cgi?id=2208
* libtiff/tif\_dirread.c: fix needless tag ordering warning http://bugzilla.maptools.org/show\_bug.cgi?id=2210
* libtiff/tif\_jpeg.c: reduce usage of JCS\_UNKNOWN in order to improve compatibility with various viewers submitted by e-mail from Dwight Kelly
* libtiff/tif\_strip.c: use TIFFGetFieldDefaulted instead of TIFFGetField when we assume that it will succeed http://bugzilla.maptools.org/show\_bug.cgi?id=2215
* libtiff/tif\_dirread.c: tolerate some cases where FIELD\_COLORMAP is missing http://bugzilla.maptools.org/show\_bug.cgi?id=2189
* libtiff/tif\_jpeg.c: Fix regressions with 2 and 3 band images caused by commit on 2010-12-14. Submitted by e-mail from Even Rouault
* libtiff/tif\_dirwrite.c: Avoid undefined behaviour when casting from float to unsigned integer in TIFFWriteRationalArray() as reported by Kareem Shehata.
* libtiff/tif\_fax3.h: Protect against a fax VL(n) codeword commanding a move left. Without this, a malicious input file can generate an indefinitely large series of runs without a0 ever reaching the right margin, thus overrunning our buffer of run lengths. Per CVE-2011-0192. This is a modified version of a patch proposed by Drew Yao of Apple Product Security. It adds an unexpected() report, and disallows the equality case, since emitting a run without increasing a0 still allows buffer overrun.
* libtiff/tif\_fax3.h: Fix to last change allowing zero length runs at the start of a scanline - needed for legal cases.
* libtiff/tif\_thunder.c: Correct potential buffer overflow with thunder encoded files with wrong bitspersample set. The libtiff development team would like to thank Marin Barbella and TippingPoint's Zero Day Initiative for reporting this vulnerability (ZDI-CAN-1004, CVE-2011-1167). http://bugzilla.maptools.org/show\_bug.cgi?id=2300
* libtiff/tiffiop.h: avoid declaring int64/uint64 on AIX with XLC where they are already available. (#2301)

**CHANGES IN THE TOOLS:**

* tools/tiffcrop.c: Patch from Richard Nolde. Reject YCbCr subsampled data since tiffcrop currently doesn't support it. Fix JPEG support.
* tools/tiffcp.c: Initialize buffer arrays with zero to avoid referencing to uninitialized memory in some cases (e.g. when tile size set bigger than the image size).
* tools/tiff2pdf.c: Better generation of ID field in t2p\_write\_pdf\_trailer(). Get rid of GCC aliasing warnings.
* tools/tiff2pdf.c: Fixed computation of the tile buffer size when converting JPEG encoded tiles.
* tools/tiff2pdf.c: Better handling of string fields, use static string buffers instead of dynamically allocated, use strncpy() instead of strcpy(), control the string lengths.
* tools/{tiff2bw.c, thumbnail.c, pal2rgb.c}: Fix the count for WhitePoint tag as per bug http://bugzilla.maptools.org/show\_bug.cgi?id=2042
* tools/tiffdump.c: Use PrintData() function instead of PrintByte/Short/Long(). Should fix an issue reported at http://bugzilla.maptools.org/show\_bug.cgi?id=2116
* tools/tiffset.c: Properly handle TIFFTAG\_PAGENUMBER, TIFFTAG\_HALFTONEHINTS, TIFFTAG\_YCBCRSUBSAMPLING, TIFFTAG\_DOTRANGE which should be set by value.
* tools/tiffdump.c: Avoid integer overflows computing the buffer size for large directories. As per bug http://bugzilla.maptools.org/show\_bug.cgi?id=2218
* tools/tiff2pdf.c: Fixed ID buffer filling in t2p\_write\_pdf\_trailer(), thanks to Dmitry V. Levin.
* tools/tiffcrop.c: Patch from Richard Nolde to avoid a potentially unterminated buffer due to using an exceptionally long file name.
* tools/tiff2ps.c: improvements and enhancements from Richard Nolde with additional command line options for Document Title, Document Creator, and Page Orientation
* tools/tiffsplit.c: abort when reading a TIFF without a byte-count per http://bugzilla.maptools.org/show\_bug.cgi?id=1996
* tools/tiff2pdf.c: add fill-page option http://bugzilla.maptools.org/show\_bug.cgi?id=2051
* tools/fax2ps.c: replace unsafe tmpfile() with mkstemp() http://bugzilla.maptools.org/show\_bug.cgi?id=2118
* tools/tiff2pdf.c: fix colors for images with RGBA interleaved data http://bugzilla.maptools.org/show\_bug.cgi?id=2250
* tools/tiffcrop.c: new release by Richard Nolde http://bugzilla.maptools.org/show\_bug.cgi?id=2004
* tools/fax2ps.c: be consistent with page-numbering http://bugzilla.maptools.org/show\_bug.cgi?id=2225
* tools/gif2tiff.c: fix buffer overrun http://bugzilla.maptools.org/show\_bug.cgi?id=2270
* tools/fax2ps.c (main): Use tmpfile() rather than mkstemp() since it is much more portable. Tmpfile is included in ISO/IEC 9899:1990 and the WIN32 CRT.

**CHANGES IN THE CONTRIB AREA:**

* None

Last updated $Date: 2016-09-25 20:05:47 $.