**TIFF CHANGE INFORMATION**

**Current Version**: v4.0.4beta  
**Previous Version**: [v4.0.3](http://docs.google.com/v4.0.3.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](#gjdgxs)
* [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:**

* Updated to use Automake 1.15 and Libtool 2.4.5

**CHANGES IN LIBTIFF:**

* TIFFCheckDirOffset(): avoid uint16 overflow when reading more than 65535 directories, and effectively error out when eaching that limit.
* TIFFNumberOfDirectories(): generate error in case of directory count overflow.
* TIFFAdvanceDirectory(): If nextdir is found to be defective, then set it to zero before returning error in order to terminate processing of truncated TIFF.
* JPEG-in-TIFF: recognize SOF2, SOF9 and SOF10 markers to avoid emitting a warning. Fix for compatibility with mozjpeg library. Note: the default settings of mozjpeg will produce progressive scans, which is forbidden by the TechNote.
* JPEG-in-TIFF: Fix regression introduced in 3.9.3/4.0.0 that caused all tiles/strips to include quantization tables even when the jpegtablesmode had the JPEGTABLESMODE\_QUANT bit set. Also add explicit removal of Huffman tables when jpegtablesmode has the JPEGTABLESMODE\_HUFF bit set, which avoids Huffman tables to be emitted in the first tile/strip (only useful in update scenarios. create-only was fine)
* JPEG-in-TIFF: fix segfault in JPEGFixupTagsSubsampling() on corrupted image where tif->tif\_dir.td\_stripoffset == NULL. ([#2471](http://bugzilla.maptools.org/show_bug.cgi?id=2471))
* NeXT codec: add new tests to check that we don't read outside of the compressed input stream buffer.
* NeXT codec: check that BitsPerSample = 2. Fixes [#2487](http://bugzilla.maptools.org/show_bug.cgi?id=2487) (CVE-2014-8129)
* NeXT codec: in the "run mode", use tilewidth for tiled images instead of imagewidth to avoid crash
* tif\_getimage.c: in OJPEG case, fix checks on strile width/height in the putcontig8bitYCbCr42tile, putcontig8bitYCbCr41tile and putcontig8bitYCbCr21tile cases.
* in TIFFDefaultDirectory(), reset any already existing extented tags installed by user code through the extender mechaninm before calling the extender callback (GDAL #5054)
* Fix warnings about unused parameters.
* Fix various typos in comments found by Debian lintian tool (GDAL #5756)
* tif\_getimage.c: avoid divide by zero on invalid YCbCr subsampling. ([#2235](http://bugzilla.maptools.org/show_bug.cgi?id=2235))
* tif\_dirread.c: In EstimateStripByteCounts(), check return code of \_TIFFFillStriles(). This solves crashing bug on corrupted images generated by afl.
* tif\_read.c: fix several invalid comparisons of a uint64 value with <= 0 by casting it to int64 first. This solves crashing bug on corrupted images generated by afl.
* TIFFSetField(): refuse to set negative values for TIFFTAG\_XRESOLUTION and TIFFTAG\_YRESOLUTION that cause asserts when writing the directory
* TIFFReadDirectory(): refuse to read ColorMap or TransferFunction if BitsPerSample has not yet been read, otherwise reading it later will cause user code to crash if BitsPerSample > 1
* TIFFRGBAImageOK(): return FALSE if LOGLUV with SamplesPerPixel != 3, or if CIELAB with SamplesPerPixel != 3 or BitsPerSample != 8
* tif\_config.vc.h: no longer use "#define snprintf \_snprintf" with Visual Studio 2015 aka VC 14 aka MSVC 1900
* LZW codec: prevent potential null dereference of sp->dec\_codetab in LZWPreDecode ([#2459](http://bugzilla.maptools.org/show_bug.cgi?id=2459))
* TIFFReadBufferSetup(): avoid passing -1 size to TIFFmalloc() if passed user buffer size is 0 ([#2459](http://bugzilla.maptools.org/show_bug.cgi?id=2459))
* TIFFReadDirEntryOutputErr(): Incorrect count for tag should be a warning rather than an error since errors terminate processing.
* tif\_dirinfo.c (TIFFField) : Fix data type for TIFFTAG\_GLOBALPARAMETERSIFD tag.
* Add definitions for TIFF/EP CFARepeatPatternDim and CFAPattern tags ([#2457](http://bugzilla.maptools.org/show_bug.cgi?id=2457))
* tif\_codec.c, tif\_dirinfo.c: Enlarge some fixed-size buffers that weren't large enough, and eliminate substantially all uses of sprintf(buf, ...) in favor of using snprintf(buf, sizeof(buf), ...)
* configure.ac: Improve pkg-config static linking by adding -lm to Libs.private when needed.
* tif\_write.c: tmsize\_t related casting warning fixed for 64bit linux.
* tif\_read.c: uint64/tmsize\_t change for MSVC warnings. ([#2427](http://bugzilla.maptools.org/show_bug.cgi?id=2427))
* Fix TIFFPrintDirectory's handling of field\_passcount fields: it had the TIFF\_VARIABLE and TIFF\_VARIABLE2 cases backwards.
* PixarLog codec: Improve previous patch for CVE-2012-4447 (to enlarge tbuf for possible partial stride at end) so that overflow in the integer addition is detected.
* tif\_{unix,vms,win32}.c (\_TIFFmalloc): ANSI C does not require malloc() to return NULL pointer if requested allocation size is zero. Assure that \_TIFFmalloc does.
* tif\_zip.c: Avoid crash on NULL error messages.

**CHANGES IN THE TOOLS:**

* tiff2pdf: Fis various crashes and memory buffer access errors (oCERT-2014-013).
* tiff2pdf: fix buffer overflow on some YCbCr JPEG compressed images. ([#2445](http://bugzilla.maptools.org/show_bug.cgi?id=2445))
* tiff2pdf: fix buffer overflow on YCbCr JPEG compressed image. ([#2443](http://bugzilla.maptools.org/show_bug.cgi?id=2443))
* tiff2pdf: check return code of TIFFGetField() when reading TIFFTAG\_SAMPLESPERPIXEL
* tiff2pdf: fix crash due to invalid tile count.
* tiff2pdf: Detect invalid settings of BitsPerSample/SamplesPerPixel for CIELAB / ITULAB
* tiff2pdf: Assure that memory size calculations for \_TIFFmalloc() do not overflow the range of tmsize\_t.
* tiff2pdf: Avoid crash when TIFFTAG\_TRANSFERFUNCTION tag returns one channel, with the other two channels set to NULL.
* tiff2pdf: close PDF file. ([#2479](http://bugzilla.maptools.org/show_bug.cgi?id=2479))
* tiff2pdf: Preserve input file directory order when pages are tagged with the same page number.
* tiff2pdf.c: terminate after failure of allocating ycbcr buffer ([#2449](http://bugzilla.maptools.org/show_bug.cgi?id=2449) CVE-2013-4232)
* tiff2pdf: Rewrite JPEG marker parsing in t2p\_process\_jpeg\_strip to be at least marginally competent. The approach is still fundamentally flawed, but at least now it won't stomp all over memory when given bogus input. Fixes CVE-2013-1960.
* tiffdump: Guard against arithmetic overflow when calculating allocation buffer sizes.
* tiffdump: fix crash due to overflow of entry count.
* tiffdump: Fix double-free bug.
* tiffdump: detect cycle in TIFF directory chaining. ([#2463](http://bugzilla.maptools.org/show_bug.cgi?id=2463))
* tiffdump: avoid passing a NULL pointer to read() if seek() failed before. ([#2459](http://bugzilla.maptools.org/show_bug.cgi?id=2459))
* tiff2bw: when Photometric=RGB, the utility only works if SamplesPerPixel = 3. Enforce that. ([#2485](http://bugzilla.maptools.org/show_bug.cgi?id=2485), CVE-2014-8127)
* pal2rgb, thumbnail: fix crash by disabling TIFFTAG\_INKNAMES copying. ([#2484](http://bugzilla.maptools.org/show_bug.cgi?id=2484), CVE-2014-8127)
* thumbnail: fix out-of-buffer write. ([#2489](http://bugzilla.maptools.org/show_bug.cgi?id=2489), CVE-2014-8128)
* thumbnail, tiffcmp: only read/write TIFFTAG\_GROUP3OPTIONS or TIFFTAG\_GROUP4OPTIONS if compression is COMPRESSION\_CCITTFAX3 or COMPRESSION\_CCITTFAX4. ([#2493](http://bugzilla.maptools.org/show_bug.cgi?id=2493), CVE-2014-8128)
* tiffcp: fix crash when converting YCbCr JPEG-compressed to none. ([#2480](http://bugzilla.maptools.org/show_bug.cgi?id=2480))
* bmp2tiff: fix crash due to int overflow related to input BMP dimensions
* tiffcrop: fix crash due to invalid TileWidth/TileHeight
* tiffcrop: fix segfault if bad value passed to -Z option ( [#2459](http://bugzilla.maptools.org/show_bug.cgi?id=2459)) and add missing va\_end in dump\_info
* thumbnail, tiffcrop: "fix" heap read over-run found with Valgrind and Address Sanitizer on test suite
* fax2ps: check malloc()/realloc() result. ([#2470](http://bugzilla.maptools.org/show_bug.cgi?id=2470))
* gif2tiff: apply patch for CVE-2013-4243. ([#2451](http://bugzilla.maptools.org/show_bug.cgi?id=2451))
* gif2tiff: fix possible OOB write. ([#2452](http://bugzilla.maptools.org/show_bug.cgi?id=2452), CVE-2013-4244)
* gif2tiff: Be more careful about corrupt or hostile input files ([#2450](http://bugzilla.maptools.org/show_bug.cgi?id=2450), CVE-2013-4231)
* tiff2rgba: fix usage message in that zip was wrongly described
* tiffinfo: Default various values fetched with TIFFGetField() to avoid being uninitialized.
* tiff2ps: Fix bug in auto rotate option code.
* ppm2tiff: avoid zero size buffer vulnerability (CVE-2012-4564). check the linebytes calculation too, get the max() calculation straight, avoid redundant error messages, check for malloc failure.
* tiffset: now supports a -u option to unset a tag. ([#2419](http://bugzilla.maptools.org/show_bug.cgi?id=2419))
* Fix warnings about unused parameters.
* rgb2ycbcr, tiff2bw, tiff2pdf, tiff2ps, tiffcrop, tiffdither : Enlarge some fixed-size buffers that weren't large enough, and eliminate substantially all uses of sprintf(buf, ...) in favor of using snprintf(buf, sizeof(buf), ...), so as to protect against overflow of fixed-size buffers. This responds in particular to CVE-2013-1961 concerning overflow in tiff2pdf.c's t2p\_write\_pdf\_page().
* html/man/tiff2ps.1.html, html/man/tiffcp.1.html, html/man/tiffdither.1.html, man/tiff2ps.1, man/tiffcp.1, man/tiffdither.1, tools/tiff2ps.c, tools/tiffcp.c, tools/tiffdither.c: Sync tool usage printouts and man pages with reality

**CHANGES IN THE CONTRIB AREA:**

* Fix warnings about variables set but not used.
* contrib/dbs/xtiff/xtiff.c: Enlarge some fixed-size buffers that weren't large enough, and eliminate substantially all uses of sprintf(buf, ...) in favor of using snprintf(buf, sizeof(buf), ...), so as to protect against overflow of fixed-size buffers.

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