**TIFF CHANGE INFORMATION**

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

* configure.ac / configure
  + Bugzilla Bug #2405: Correct shell equality operator.
  + Bugzilla Bug #2498: Adds an option to select the file I/O style on Windows hosts.

**CHANGES IN LIBTIFF:**

* tif\_dir.c:
  + TIFFNumberOfDirectories: Coverity 1134470 "Logically dead code"
* tif\_dirread.c:
  + TIFFReadDirEntryDoubleArray: Coverity 298626 "Logically dead code".
  + TIFFReadDirEntryFloatArray: Coverity 298627 "Logically dead code".
  + TIFFReadDirEntryIfd8Array: Coverity 298628 "Logically dead code".
  + TIFFReadDirEntrySlong8Array: Coverity 298629 "Logically dead code"
* tif\_dirwrite.c
  + \_TIFFRewriteField: Coverity 1024310 "Resource leak".
* tif\_jpeg.c
  + JPEGCleanup: Coverity 298624 "Dereference before null check".
  + JPEGDecode: Coverity 602597 "Operands don't affect result".
* tif\_getimage.c
  + Bugzilla Bug #2409: Correct reading of certain tiled TIFFs.
* tif\_luv.c
  + LogLuvDecodeStrip: Coverity 991239 "Division or modulo by zero".
  + LogLuvDecodeTile: Coverity 991227 "Division or modulo by zero".
  + LogLuvEncodeStrip: Coverity 991240 "Division or modulo by zero".
  + LogLuvEncodeTile: Coverity 991241 "Division or modulo by zero".
* tif\_lzw.c
  + Decode files that contain consecutive CODE\_CLEAR codes.
* tif\_ojpeg.c
  + OJPEGReadBufferFill: Coverity 603400 "Missing break in switch".
  + OJPEGReadHeaderInfoSecStreamDht: Coverity 601720 "Resource leak".
* tif\_read.c
  + TIFFStartTile: Coverity 715973 and 715974 "Division or modulo by zero".
* tif\_unix.c
  + Bugzilla Bug #2510: Fix several harmless but still annoying warnings.
* tif\_write
  + TIFFWriteEncodedStrip: Coverity 715975 "Division or modulo by zero".
  + TIFFWriteEncodedTile: Coverity 715976 and 715977 "Division or modulo by zero".
  + TIFFWriteRawStrip: Coverity 715978 "Division or modulo by zero".
  + TIFFWriteScanline: Coverity 715979 "Division or modulo by zero".

**CHANGES IN THE TOOLS:**

* bmp2tiff
  + Coverity 1024225 "Untrusted value as argument".
  + Coverity 1024678 "Unchecked return value from library".
  + Coverity 1024679 "Unchecked return value from library".
  + Coverity 1214160 "Ignoring number of bytes read".
* gif2tiff
  + Coverity 1024222 "Untrusted value as argument".
  + Coverity 1024890 "Ignoring number of bytes read".
  + Coverity 1024891 "Ignoring number of bytes read".
  + Coverity 1024892 "Ignoring number of bytes read".
  + Coverity 1024893 "Ignoring number of bytes read".
  + Coverity 1024894 "Ignoring number of bytes read".
* ras2tiff
  + Corrected Sun Raster header definition to be safe for 64-bit systems. Add some header validations. Fixes many (unspecified) Coverity issues.
  + Coverity 1024223 "Untrusted value as argument".
  + Coverity 1301206: "Integer handling issues (BAD\_SHIFT)".
* raw2tiff
  + Coverity 1024887 "Unchecked return value from library".
  + Coverity 1024888 "Unchecked return value from library".
  + Coverity 1024889 "Unchecked return value from library".
  + Coverity 1214162 "Ignoring number of bytes read".
* tiff2pdf
  + Bugzilla Bug #2078. Suppress initial output of the header.
  + Bugzilla Bug #2150. Change ColorTransform from "0" to "1".
  + Take care in using the return value from snprintf().
  + Coverity 1024181 "Structurally dead code".
  + Coverity 1024181 "Structurally dead code".
  + Coverity 1227690 "Unused value".
  + Coverity 298621 "Resource leak".
* tiff2ps
  + Correct sizing and scaling problems with output document.
* tiffcp
  + Coverity 1024306, 1024307, 1024308, 1024309 "Resource leak".
* tiffcrop
  + Correctly copy the compression tag from the source TIFF.
  + Coverity 1024545 "Division or modulo by zero".
  + Coverity 1024586 "Logically dead code".
  + Coverity 1024796 "Nesting level does not match indentation".
  + Coverity 1024797 "Nesting level does not match indentation".
  + Coverity 1294542 "Logical vs. bitwise operator".
  + Coverity 1299740 "Out-of-bounds write".
  + Coverity 1299741 "Dereference before null check".
* tiffdither
  + Check memory allocations for failure. Also check multiplication overflow. (Fixes #2501, CVE-2014-8128)
* tiffgt.c
  + Bugzilla Bug #2401. Appropriately call glFlush().
* tiffmedian
  + Coverity 1024386 "Out-of-bounds read".
  + Coverity 1024386 "Out-of-bounds read".
  + Coverity 1024795 "Nesting level does not match indentation".
  + Coverity 1024795 "Nesting level does not match indentation".
* tiffsplit
  + Coverity 1024304 "Resource leak".
  + Coverity 1024305 "Resource leak".

**CHANGES IN THE CONTRIB AREA:**

* addtiffo
  + Check buffer size calculation for overflow.
  + Coverity 298615 "Resource leak".
  + Coverity 1024649 "Unintended sign extension".
* iptcutil
  + Coverity 1024468 "Infinite loop".
  + Coverity 1024727 "Truncated stdio return value".
  + Coverity 1214240 "Untrusted loop bound".

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