Bug 2656 - Heap based buffer overflow in tools/tiffcp

Status: RESOLVED FIXED
Reported: 2017-01-06 06:56 by Li Yuekang
Modified: 2017-01-11 14:27 (History)

Product: libtiff
Component: default
Version: unspecified
Platform: PC Linux

Importance: P2 critical
Target Milestone: ---
Assigned To: Frank Warmerdam

URL:
Whiteboard:
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

Attachments	
the bug report and poc (1.24 KB, application/zip) 2017-01-06 06:59, Li Yuekang	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.

Description From Li Yuekang 2017-01-06 06:56:51

```
A bug report and a PoC are as in the attachment.

The stacktrace:
==17449==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xb58006a0 at
pc 0x0804d903 bp 0xbfeb5068 sp 0xbfeb5058
READ of size 1 at 0xb58006a0 thread T0
    #0 0x804d902 in cpContig2SeparateByRow
/home/lyk/tiff-4.0.7-asan/tools/tiffcp.c:1091
    #1 0x804b31d in tiffcp /home/lyk/tiff-4.0.7-asan/tools/tiffcp.c:815
    #2 0x804b31d in main /home/lyk/tiff-4.0.7-asan/tools/tiffcp.c:304
    #3 0xb6fd0636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)
    #4 0x804c81b  (/home/lyk/inscmp/afl-2.33b/test/tiffcp_a+0x804c81b)
```

------- Comment #1 From Li Yuekang 2017-01-06 06:59:38 -------

Created an attachment (id=742) [details]
the bug report and poc

------- Comment #2 From Li Yuekang 2017-01-06 07:04:36 -------

Forgot to say :p, the version is 4.0.7

------- *Comment #3 From Li Yuekang 2017-01-09 02:26:41* -------

There is a sister bug (~~bug 2657~~) for this one
~~http://bugzilla.maptools.org/show_bug.cgi?id=2657~~

------- *Comment #4 From Even Rouault 2017-01-11 14:27:03* -------

Fixed per

2017-01-11 Even Rouault <even.rouault at spatialys.com>

        * 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~~

less C/cvs/maptools/cvsroot/libtiff/ChangeLog,v <-- ChangeLog
new revision: 1.1210; previous revision: 1.1209
/cvs/maptools/cvsroot/libtiff/tools/tiffcp.c,v <-- tools/tiffcp.c
new revision: 1.61; previous revision: 1.60

First Last Prev Next No search results available Format For Printing - XML - Clone This Bug - Top of page