Bug 2657 - Heap based buffer overflow in tools/tiffcp

Status: RESOLVED FIXED

Reported: 2017-01-09 00:07 by Li Yuekang

Modified: 2017-01-11 14:27 (History)

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

Importance: P1 enhancement
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) 2017-01-09 00:07, 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 2017-01-09 00:07:17

Created an attachment (id=743) [details]
the bug report and poc

This is a bug similar to ~~Bug 2656~~.
(~~http://bugzilla.maptools.org/show_bug.cgi?id=2656~~)

------- *Comment #1 From Even Rouault 2017-01-11 14:27:13* -------

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