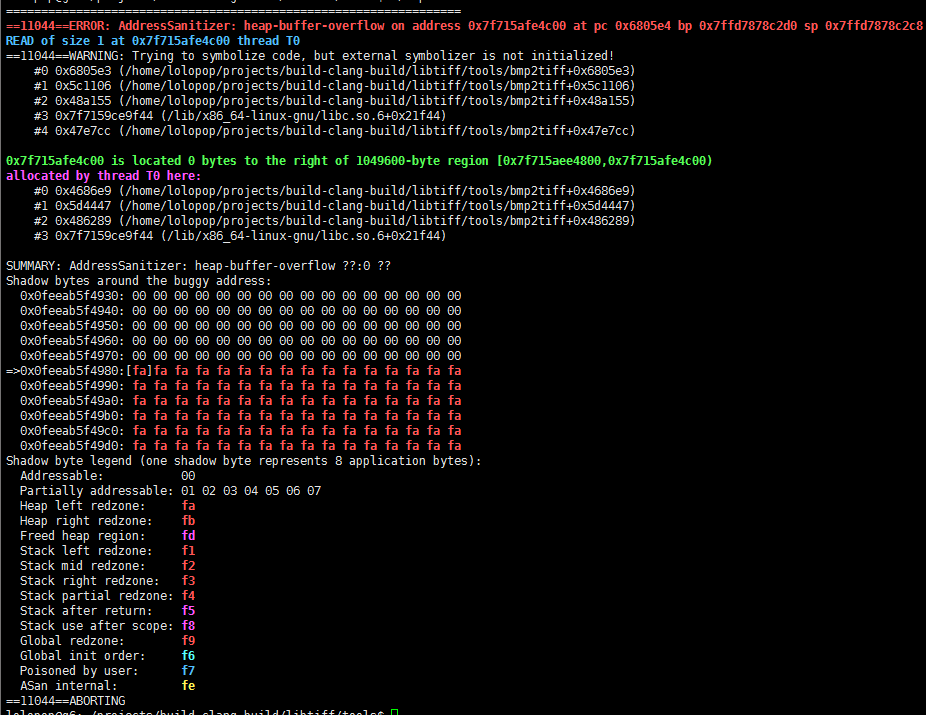
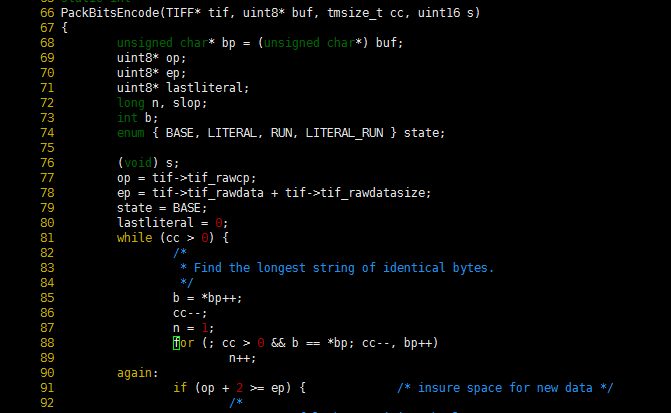
Exception

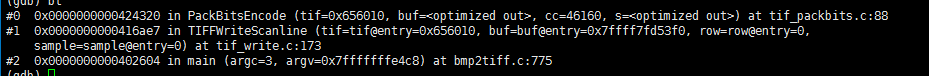


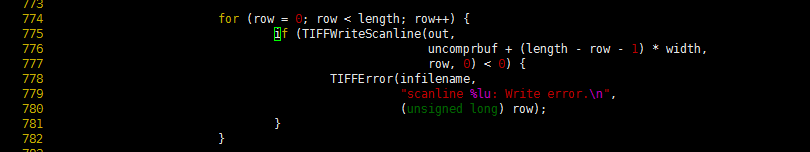
As above shown, this is a heap buffer overflow vulnerability.

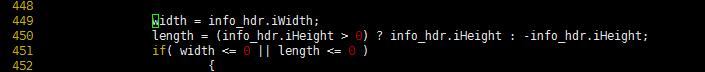
Main Reason:

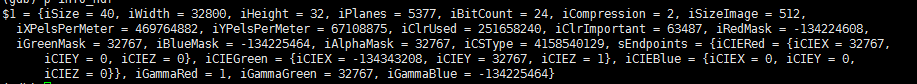
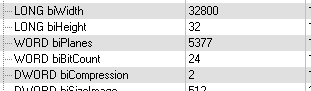
Did not check the user input BMP file. The program does not check for biWidth and biHeight in bitmap-information header. The biWidth and biHeight do not match the actual input of the bmp image causing the heap buffer overflow.

By looking at the source code, the value of the pointer bp is obtained by the pointer buf.

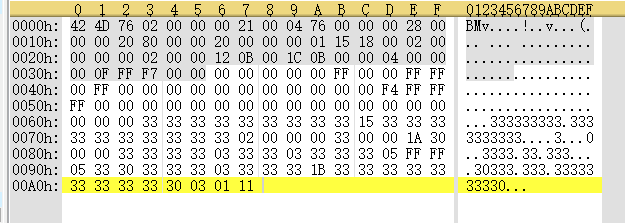
Through traceability, the value of the pointer buf is defined in the TIFFWriteScanline function in tif\_write.c. The call to the TIFFWriteScanline function is in bmp2tiff.c.

By looking at the bmp2tiff.c file source code, the length of Buf is determined by uncomprbuf + (length-row-1) \* width. In line 449 of bmp2tiff.c, width and length are assigned.



By setting a breakpoint on this place, we found Width = 32800 length = 32.  
By opening the crash1.bmp with 010 Editor.exe, the values ​​of Width and length are consistent with the bitmap-information header

But the crash1.bmp file is very small . The whole contents are as follows



This will cause the program crosses the border to read the memory, causing the vulnerability to trigger.

**Author**

Name: Rong Chenghao

Org: IIE (http:// iie.ac.cn)