CVE-2017-5508

描述：Heap-based buffer overflow in the PushQuantumPixel function in ImageMagick before 6.9.7-3 and 7.x before 7.0.4-3 allows remote attackers to cause a denial of service (application crash) via a crafted TIFF file.

软件：ImageMagick

源码：coders/tiff.c

出现位置： 1606-1613行

关键源码：

method=ReadTileMethod;

quantum\_info->endian=LSBEndian;

quantum\_type=RGBQuantum;

- tiff\_pixels=(unsigned char \*) AcquireMagickMemory(TIFFScanlineSize(tiff)+

- sizeof(uint32));

+ tiff\_pixels=(unsigned char \*) AcquireMagickMemory(MagickMax(

+ TIFFScanlineSize(tiff),(size\_t) (image->columns\*samples\_per\_pixel\*

+ pow(2.0,ceil(log(bits\_per\_sample)/log(2.0))))));

if (tiff\_pixels == (unsigned char \*) NULL)

{

TIFFClose(tiff);