CVE-2016-7525

描述：Heap-based buffer overflow in coders/psd.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PSD file.

软件：ImageMagick

源码：[coders/psd.c](https://github.com/ImageMagick/ImageMagick/commit/5f16640725b1225e6337c62526e6577f0f88edb8" \l "diff-57d2cedbdffead46c821c7b3601b3464" \o "coders/psd.c)

出现位置： 575-582 918-922行

关键源码：

static inline size\_t GetPSDRowSize(Image \*image)

{

if (image->depth == 1)

return((image->columns+7)/8);

else

return(image->columns\*GetPSDPacketSize(image));

}

row\_size=GetPSDRowSize(image);

pixels=(unsigned char \*) AcquireQuantumMemory(row\_size,sizeof(\*pixels));

if (pixels == (unsigned char \*) NULL)

ThrowBinaryException(ResourceLimitError,"MemoryAllocationFailed",

image->filename);