CVE-2017-5511

描述：coders/psd.c in ImageMagick allows remote attackers to have unspecified impact by leveraging an improper cast, which triggers a heap-based buffer overflow.

软件：ImageMagick

源码：coders/psd.c

出现位置： 1671-1678行

关键源码：

@@ -1671,7 +1671,7 @@ ModuleExport MagickBooleanType ReadPSDLayers(Image \*image,

/\*

Layer name.

\*/

- length=(MagickSizeType) ReadBlobByte(image);

+ length=(MagickSizeType) (unsigned char) ReadBlobByte(image);

combined\_length+=length+1;

if (length > 0)

(void) ReadBlob(image,(size\_t) length++,layer\_info[i].name);