CVE-2016-10066

描述：Buffer overflow in the ReadVIFFImage function in coders/viff.c in ImageMagick before 6.9.4-5 allows remote attackers to cause a denial of service (application crash) via a crafted file.

软件：ImageMagick

源码：coders/aai.c

出现位置： 158-162行

关键源码：

if ((image\_info->ping != MagickFalse) && (image\_info->number\_scenes != 0))

if (image->scene >= (image\_info->scene+image\_info->number\_scenes-1))

break;

pixels=(unsigned char \*) AcquireQuantumMemory(image->columns,

4\*sizeof(\*pixels));