CVE-2016-7520

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

软件：ImageMagick-7.0.1-0

源码：coders/hdr.c

出现位置： 722-750行

关键源码：

if (image->gamma != 0.0)

{

count=FormatLocaleString(header,MagickPathExtent,"GAMMA=%g\n",

image->gamma);

(void) WriteBlob(image,(size\_t) count,(unsigned char \*) header);

}

count=FormatLocaleString(header,MagickPathExtent,

"PRIMARIES=%g %g %g %g %g %g %g %g\n",

image->chromaticity.red\_primary.x,image->chromaticity.red\_primary.y,

image->chromaticity.green\_primary.x,image->chromaticity.green\_primary.y,

image->chromaticity.blue\_primary.x,image->chromaticity.blue\_primary.y,

image->chromaticity.white\_point.x,image->chromaticity.white\_point.y);

(void) WriteBlob(image,(size\_t) count,(unsigned char \*) header);

length=CopyMagickString(header,"FORMAT=32-bit\_rle\_rgbe\n\n",MagickPathExtent);

(void) WriteBlob(image,length,(unsigned char \*) header);

count=FormatLocaleString(header,MagickPathExtent,"-Y %.20g +X %.20g\n",

(double) image->rows,(double) image->columns);

(void) WriteBlob(image,(size\_t) count,(unsigned char \*) header);

/\*

Write HDR pixels.

\*/

pixels=(unsigned char \*) AcquireQuantumMemory(image->columns+128,4\*

sizeof(\*pixels));

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

ThrowWriterException(ResourceLimitError,"MemoryAllocationFailed");

(void) ResetMagickMemory(pixels,0,4\*(image->columns+128)\*sizeof(\*pixels));

for (y=0; y < (ssize\_t) image->rows; y++)