CVE-2016-7521

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： 487-492行

关键源码：

length++;

for (j=0; j < (ssize\_t) length; j++)

{

+ CheckNumberCompactPixels;

switch (depth)

{

case 1:

{

CheckNumberPixels(8);

\*pixels++=(\*compact\_pixels >> 7) & 0x01 ? 0U : 255U;

\*pixels++=(\*compact\_pixels >> 6) & 0x01 ? 0U : 255U;

\*pixels++=(\*compact\_pixels >> 5) & 0x01 ? 0U : 255U;

\*pixels++=(\*compact\_pixels >> 4) & 0x01 ? 0U : 255U;

\*pixels++=(\*compact\_pixels >> 3) & 0x01 ? 0U : 255U;

\*pixels++=(\*compact\_pixels >> 2) & 0x01 ? 0U : 255U;

\*pixels++=(\*compact\_pixels >> 1) & 0x01 ? 0U : 255U;

\*pixels++=(\*compact\_pixels >> 0) & 0x01 ? 0U : 255U;

break;

}