CVE-2017-7863

描述：FFmpeg before 2017-02-04 has an out-of-bounds write caused by a heap-based buffer overflow related to the decode\_frame\_common function in libavcodec/pngdec.c.

软件：FFmpeg

源码：libavcodec/pngdec.c

出现位置： 1243-1258行

关键源码：

for (y = 0; y < s->height; ++y) {

uint8\_t \*row = &s->image\_buf[s->image\_linesize \* y];

/\* since we're updating in-place, we have to go from right to left \*/

for (x = s->width; x > 0; --x) {

uint8\_t \*pixel = &row[s->bpp \* (x - 1)];

memmove(pixel, &row[raw\_bpp \* (x - 1)], raw\_bpp);

if (!memcmp(pixel, s->transparent\_color\_be, raw\_bpp)) {

memset(&pixel[raw\_bpp], 0, byte\_depth);

} else {

memset(&pixel[raw\_bpp], 0xff, byte\_depth);

}

}