CVE-2017-7866

描述：FFmpeg before 2017-01-23 has an out-of-bounds write caused by a stack-based buffer overflow related to the decode\_zbuf function in libavcodec/pngdec.c.

软件：FFmpeg before 2017-01-23

源码：libavcodec/pngdec.c.

出现位置： 445-457行

关键源码：

zstream.next\_out = buf;

zstream.avail\_out = buf\_size;

ret = inflate(&zstream, Z\_PARTIAL\_FLUSH);

if (ret != Z\_OK && ret != Z\_STREAM\_END) {

ret = AVERROR\_EXTERNAL;

goto fail;

}

bp->len += zstream.next\_out - buf;

if (ret == Z\_STREAM\_END)

break;

}

inflateEnd(&zstream);

bp->str[bp->len] = 0;

数组越界