CVE-2017-8363

描述：The flac\_buffer\_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted audio file.

软件： libsndfile 1.0.28

源码： src/flac.c

出现位置： 266-267行

关键源码：

for (i = 0 ; i < len && pflac->remain > 0 ; i++)

{ offset = pflac->pos + i \* channels ;

if (pflac->bufferpos >= frame->header.blocksize)

break ;

if (offset + channels > pflac->len)

break ;

for (j = 0 ; j < channels ; j++)

retpcm [offset + j] = ((uint32\_t) buffer [j][pflac->bufferpos]) << shift ;

pflac->remain -= channels ;

pflac->bufferpos++ ;

} ;