CVE-2017-7585

描述：In libsndfile before 1.0.28, an error in the "flac\_buffer\_copy()" function (flac.c) can be exploited to cause a stack-based buffer overflow via a specially crafted FLAC file.

软件：libsndfile

源码：src/flac.c

出现位置： 188-204行

关键源码：

if (pflac->ptr == NULL)

{ /\*

\*\* Not sure why this code is here and not elsewhere.

\*\* Removing it causes valgrind errors.

\*/

pflac->bufferbackup = SF\_TRUE ;

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

{

if (pflac->rbuffer [i] == NULL)

pflac->rbuffer [i] = calloc (FLAC\_\_MAX\_BLOCK\_SIZE, sizeof (int32\_t)) ;

memcpy (pflac->rbuffer [i], buffer [i], frame->header.blocksize \* sizeof (int32\_t)) ;

} ;

pflac->wbuffer = (const int32\_t\* const\*) pflac->rbuffer ;

return 0 ;

} ;