CVE-2017-8365

描述：The i2les\_array function in pcm.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file.

软件：libsndfile 1.0.28

源码：src/pcm.c

出现位置： 670行

关键源码：

i2les\_array (const int \*src, short \*dest, int count)

{ unsigned char \*ucptr ;

ucptr = ((unsigned char\*) dest) + 2 \* count ;

while (--count >= 0) //循环复制

{ ucptr -= 2 ;

ucptr [0] = src [count] >> 16 ;

ucptr [1] = src [count] >> 24 ;

} ;