CVE-2017-6831

描述：Heap-based buffer overflow in the decodeBlockWAVE function in IMA.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.

软件：audiofile-0.3.6

源码：libaudiofile/modules/IMA.cpp

出现位置： 184-191行

关键源码：

for (int s=0; s<4; s++)

{

\*output = decodeSample(m\_adpcmState[c], \*encoded & 0xf);

output += channelCount;

\*output = decodeSample(m\_adpcmState[c], \*encoded >> 4);

output += channelCount;

encoded++;

}