CVE-2017-6832

描述：Heap-based buffer overflow in the decodeBlock in MSADPCM.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/MSADPCM.cpp

出现位置： 211-226行

关键源码：

循环复制，无边界检查

while (samplesRemaining > 0)

{

uint8\_t code;

int16\_t newSample;

code = \*encoded >> 4;

newSample = decodeSample(\*state[0], code, coefficient[0]);

\*decoded++ = newSample;

code = \*encoded & 0x0f;

newSample = decodeSample(\*state[1], code, coefficient[1]);

\*decoded++ = newSample;

encoded++;

samplesRemaining -= 2;

}