CVE-2017-6830

描述：Heap-based buffer overflow in the alaw2linear\_buf function in G711.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/G711.cpp

出现位置： 51-55行

关键源码：

static void alaw2linear\_buf (const uint8\_t \*alaw, int16\_t \*linear, int nsamples)

{

for (int i=0; i < nsamples; i++)

linear[i] = \_af\_alaw2linear(alaw[i]); //循环复制

}