CVE-2017-6834

描述：Heap-based buffer overflow in the ulaw2linear\_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： 42行 206行

关键源码：

static void ulaw2linear\_buf (const uint8\_t \*ulaw, int16\_t \*linear, int nsamples)

{

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

linear[i] = \_af\_ulaw2linear(ulaw[i]);

}

if (m\_track->f.compressionType == AF\_COMPRESSION\_G711\_ULAW)

ulaw2linear\_buf(static\_cast<const uint8\_t \*>(m\_inChunk->buffer),