CVE-2017-6828

描述：Heap-based buffer overflow in the readValue function in FileHandle.cpp in audiofile (aka libaudiofile and Audio File Library) 0.3.6 allows remote attackers to have unspecified impact via a crafted WAV file.

软件：Audio File Library- 0.3.6

源码：libaudiofile/FileHandle.cpp

出现位置： 353行

关键源码：

template <typename T>

static bool readValue(File \*f, T \*value)

{

return f->read(value, sizeof (\*value)) == sizeof (\*value);

}