CVE-2017-6827

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

软件：audiofile 0.3.6

源码：libaudiofile/modules/MSADPCM.cpp

出现位置： 366-375行

关键源码：

void \*v;

if (\_af\_pv\_getptr(pv, \_AF\_MS\_ADPCM\_COEFFICIENTS, &v))

{

memcpy(m\_coefficients, v, m\_numCoefficients \* 2 \* sizeof (int16\_t));

}

else

{

\_af\_error(AF\_BAD\_CODEC\_CONFIG, "coefficient array not set");

return false;

}