CVE-2016-9264

描述：Buffer overflow in the printMP3Headers function in listmp3.c in Libming 0.4.7 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mp3 file.

软件：Libming 0.4.7

源码： util/listmp3.c

出现位置： 126-139行

关键源码：

if(version == 1)

{

samplerate = mp1\_samplerate\_table[samplerate\_idx];

if(layer == 1)

bitrate = mp1l1\_bitrate\_table[bitrate\_idx];

else if(layer == 2)

bitrate = mp1l2\_bitrate\_table[bitrate\_idx];

else if(layer == 3)

bitrate = mp1l3\_bitrate\_table[bitrate\_idx];

}