CVE-2016-9829

描述：Heap-based buffer overflow in the parseSWF\_DEFINEFONT function in parser.c in the listswf tool in libming 0.4.7 allows remote attackers to have unspecified impact via a crafted SWF file.

软件：libming 0.4.7

源码：util/parser.c

出现位置： 1655-1659行

关键源码：

parserrec->OffsetTable = (UI16 \*)malloc((firstOffset/2) \* sizeof( UI16 ) );

parserrec->OffsetTable[0] = firstOffset;

for(i=1;i<firstOffset/2;i++) {

parserrec->OffsetTable[i] = readUInt16 (f);

}