CVE-2016-9831

描述：Heap-based buffer overflow in the parseSWF\_RGBA 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： 63-70行 800-805行

关键源码：

void

parseSWF\_RGBA (FILE \* f, struct SWF\_RGBA \*rgb)

{

rgb->red = readUInt8 (f);

rgb->green = readUInt8 (f);

rgb->blue = readUInt8 (f);

rgb->alpha = readUInt8 (f);

}

.....

fillstyle->FillStyles =

(SWF\_MORPHFILLSTYLE \*) calloc (count, sizeof (SWF\_MORPHFILLSTYLE));

for (i = 0; i < count; i++)

{

parseSWF\_MORPHFILLSTYLE (f, &(fillstyle->FillStyles[i]));

}