CVE-2017-8325

描述：The iw\_process\_cols\_to\_intermediate function in imagew-main.c in libimageworsener.a in ImageWorsener before 1.3.1 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image.

软件：ImageWorsener 1.3.0

源码： src/imagew-main.c

出现位置： 901-907行

关键源码：

for(j=0;j<ctx->intermed\_canvas\_height;j++) {  
 if(is\_alpha\_channel) {  
 ctx->intermediate\_alpha32[((size\_t)j)\*ctx->intermed\_canvas\_width + i] = (iw\_float32)out\_pix[j];  
 }  
 else {  
 ctx->intermediate32[((size\_t)j)\*ctx->intermed\_canvas\_width + i] = (iw\_float32)out\_pix[j];  
 }  
}