CVE-2017-5994

描述：Heap-based buffer overflow in the vrend\_create\_vertex\_elements\_state function in vrend\_renderer.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and crash) via the num\_elements parameter.

软件：virglrenderer

源码：src/vrend\_renderer.c

出现位置： 1656-1662行

关键源码：

v->count = num\_elements;

for (i = 0; i < num\_elements; i++) {

memcpy(&v->elements[i].base, &elements[i], sizeof(struct pipe\_vertex\_element));