CVE-2017-5957

描述：Stack-based buffer overflow in the vrend\_decode\_set\_framebuffer\_state function in vrend\_decode.c in virglrenderer before 926b9b3460a48f6454d8bbe9e44313d86a65447f, as used in Quick Emulator (QEMU), allows a local guest users to cause a denial of service (application crash) via the "nr\_cbufs" argument.

软件：VirGL virtual OpenGL renderer

源码：src/vrend\_decode.c

出现位置： 136-142行

关键源码：

if (length != (2 + nr\_cbufs))

return EINVAL;

for (i = 0; i < nr\_cbufs; i++)

surf\_handle[i] = get\_buf\_entry(ctx, VIRGL\_SET\_FRAMEBUFFER\_STATE\_CBUF\_HANDLE(i)); //overflow

vrend\_set\_framebuffer\_state(ctx->grctx, nr\_cbufs, surf\_handle, zsurf\_handle);