CVE-2017-5581

描述：Buffer overflow in the ModifiablePixelBuffer::fillRect function in TigerVNC before 1.7.1 allows remote servers to execute arbitrary code via an RRE message with subrectangle outside framebuffer boundaries.

软件：TigerVNC

源码：common/rfb/PixelBuffer.cxx

出现位置： 112-140行

buf = getBufferRW(r, &stride);

if (b == 1) {

while (h--) {

memset(buf, \*(const U8\*)pix, w);

buf += stride \* b;

}

} else {

U8 \*start;

int w1;

start = buf;

w1 = w;

while (w1--) {

memcpy(buf, pix, b);

buf += b;

}

buf += (stride - w) \* b;

h--;

while (h--) {

memcpy(buf, start, w \* b);

buf += stride \* b;

}

}

commitBufferRW(r);

}