CVE-2017-6209

描述：Stack-based buffer overflow in the parse\_identifier function in tgsi\_text.c in the TGSI auxiliary module in the Gallium driver in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and QEMU process crash) via vectors related to parsing properties.

软件：VirGL virtual OpenGL renderer

源码：tgsi\_text.c

出现位置： 183-196行

关键源码：

static boolean parse\_identifier( const char \*\*pcur, char \*ret )

{

const char \*cur = \*pcur;

int i = 0;

if (is\_alpha\_underscore( cur )) {

ret[i++] = \*cur++;

while (is\_alpha\_underscore( cur ) || is\_digit( cur ))

ret[i++] = \*cur++;

ret[i++] = '\0';

\*pcur = cur;

return TRUE;

}

return FALSE;

}

//As the 'ret' has a fixed-size buffer, if the '\*pcur' has a long string,there will be a buffer overflow. This patch avoid this.