CVE-2017-7862

描述：

软件：FFmpeg

源码：libavcodec/pictordec.c

出现位置： 145-163行

关键源码：

if (s->width != avctx->width && s->height != avctx->height) {

ret = ff\_set\_dimensions(avctx, s->width, s->height);

if (ret < 0)

return ret;

}

if ((ret = ff\_get\_buffer(avctx, frame, 0)) < 0)

return ret;

memset(frame->data[0], 0, s->height \* frame->linesize[0]);

frame->pict\_type = AV\_PICTURE\_TYPE\_I;

frame->palette\_has\_changed = 1;

pos\_after\_pal = bytestream2\_tell(&s->g) + esize;

palette = (uint32\_t\*)frame->data[1];

if (etype == 1 && esize > 1 && bytestream2\_peek\_byte(&s->g) < 6) {

int idx = bytestream2\_get\_byte(&s->g);

npal = 4;

for (i = 0; i < npal; i++)

palette[i] = ff\_cga\_palette[ cga\_mode45\_index[idx][i] ];