CVE-2016-7970

描述：Buffer overflow in the calc\_coeff function in libass/ass\_blur.c in libass before 0.13.4 allows remote attackers to cause a denial of service via unspecified vectors.

软件：libass 0.13.3

源码：libass/ass\_blur.c

出现位置： 747-749行

关键源码：

- double mat\_freq[13];

+ double mat\_freq[14];

memcpy(mat\_freq, kernel, sizeof(kernel));

memset(mat\_freq + 4, 0, sizeof(mat\_freq) - sizeof(kernel));