CVE-2017-7864

描述：FreeType 2 before 2017-02-02 has an out-of-bounds write caused by a heap-based buffer overflow related to the tt\_size\_reset function in truetype/ttobjs.c.

软件：freetype2-VER-2-7-1

源码：src/truetype/ttobjs.c

出现位置： 1194-1204行

关键源码：

FT\_Size\_Metrics\* metrics;

- size->ttmetrics.valid = FALSE;

-

face = (TT\_Face)size->root.face;

+ /\* nothing to do for CFF2 \*/

+ if ( face->isCFF2 )

+ return FT\_Err\_Ok;

+

+ size->ttmetrics.valid = FALSE;

+

metrics = &size->metrics;

/\* copy the result from base layer \*/