CVE-2017-7857

描述：FreeType 2 before 2017-03-08 has an out-of-bounds write caused by a heap-based buffer overflow related to the TT\_Get\_MM\_Var function in truetype/ttgxvar.c and the sfnt\_init\_face function in sfnt/sfobjs.c.

软件：freetype2-VER-2-7.tar.gz

源码：src/sfnt/sfobjs.c

出现位置： 1058-1066行

关键源码：

@@ -1058,8 +1058,10 @@

FT\_FREE( default\_values );

FT\_FREE( instance\_values );

- /\* we don't support Multiple Master CFFs yet \*/

+ /\* we don't support Multiple Master CFFs yet; \*/

+ /\* note that `glyf' or `CFF2' have precedence \*/

if ( face->goto\_table( face, TTAG\_glyf, stream, 0 ) &&

+ face->goto\_table( face, TTAG\_CFF2, stream, 0 ) &&

!face->goto\_table( face, TTAG\_CFF, stream, 0 ) )

num\_instances = 0;