CVE-2016-10328

描述：FreeType 2 before 2016-12-16 has an out-of-bounds write caused by a heap-based buffer overflow related to the cff\_parser\_run function in cff/cffparse.c.

软件：FreeType 2

源码：cff/cffparse.c

出现位置： 1422-1435行

关键源码：

@@ -1422,13 +1422,17 @@

/\* and look for it in our current list. \*/

FT\_UInt code;

- FT\_UInt num\_args = (FT\_UInt)

- ( parser->top - parser->stack );

+ FT\_UInt num\_args;

const CFF\_Field\_Handler\* field;

+ if ( (FT\_UInt)( parser->top - parser->stack ) >= parser->stackSize )

+ goto Stack\_Overflow;

+

+ num\_args = (FT\_UInt)( parser->top - parser->stack );

\*parser->top = p;

- code = v;

+ code = v;

+

if ( v == 12 )

{

/\* two byte operator \*/