

another SEGV in FT_Set_Char_Size

Like [#1139 \(closed\)](#), I continue running with the following code and the newest commit:

```
#include "ft2build.h"
#include FT_FREETYPE_H


int main (int argc, char **argv) {
    FT_Library lib;
    FT_Face face;

    if (FT_Init_FreeType(&lib)) return 0;
    if (FT_New_Face(lib, argv[1], -3674092871004140285, &face)) return 0;
    if (FT_Set_Char_Size(face, 57705668760568013, 216172782127219456, 50384131, 3439525888)) return
}
```

and here is the file [testface](#). This time `FT_New_Face()` still returns 0, and `FT_Set_Char_Size` still throws SIGSEGV signal... Is this the third bug?

```
AddressSanitizer:DEADLYSIGNAL
=====
==611111==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000050 (pc 0x7f08d773f9bc bp 0x7f
==611111==The signal is caused by a READ memory access.
==611111==Hint: address points to the zero page.
#0 0x7f08d773f9bc in FT_Request_Size
#1 0x7f08d77401ee in FT_Set_Char_Size
#2 0x4c6cac in main
#3 0x7f08d71360b2 in __libc_start_main
#4 0x41c30d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV in FT_Request_Size
==611111==ABORTING
```

 Drag your designs here or [click to upload](#).

Tasks  0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items   0

Activity

 **Werner Lemberg** closed via commit [0c2bdb01](#) 8 months ago



Werner Lemberg @wl · 8 months ago

Owner

It's a bug, yes, now fixed. Thanks again!



Werner Lemberg mentioned in commit [0c2bdb01](#) 8 months ago



Werner Lemberg added [Bug](#) [Crash](#) labels 7 months ago



ABHISHEK PALIWAL mentioned in issue [#1138 \(closed\)](#) 6 months ago

Please [register](#) or [sign in](#) to reply