COMMUNITY CONTENT

Submit #780558: nothings stb (stb_truetype.h) ≤ 1.26 Out-of-Bounds Read

Title	nothings stb (stb_truetype.h) ≤ 1.26 Out-of-Bounds Read
Description	A heap buffer overflow (out-of-bounds read) vulnerability exists in `stbtt_InitFont_internal()` in stb_truetype.h v1.26 and earlier. The function `ttUSHORT()` at line 1286 reads 2 bytes from the font data buffer without validating that the offset is within the buffer bounds. When processing a crafted TrueType/OpenType font file with malformed table directory entries, the read exceeds the allocated buffer boundary. The vulnerability is triggered during font initialization when parsing the cmap table entries. Any application that calls `stbtt_InitFont()` on untrusted font data is affected. 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 ```
Source	⚠ https://gist.github.com/d0razi/cb31a92f3205a4373f19b7da25946848
User	d0razi (UID 96474)
Submission	03/16/2026 01:11 AM (17 days ago)
Moderation	04/01/2026 02:40 PM (17 days later)
Status	Accepted
VulDB entry	354646 [Nothings stb up to 1.26 TTF File stb_truetype.h stbtt_InitFont_internal out-of-bounds]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling