

[Sign Up](#)[Join or Log Into Facebook](#) ▼

CVE-2025-27363

Description: An out of bounds write exists in FreeType versions 2.13.0 and below (newer versions of FreeType are not vulnerable) when attempting to parse font subglyph structures related to TrueType GX and variable font files. The vulnerable code assigns a signed short value to an unsigned long and then adds a static value causing it to wrap around and allocate too small of a heap buffer. The code then writes up to 6 signed long integers out of bounds relative to this buffer. This may result in arbitrary code execution. This vulnerability may have been exploited in the wild.

Affected Version Information:

- FreeType (FreeType)
 - Default Status: unaffected
 - affected from 0.0.0 through 2.13.0

Last Updated: 2025-03-13

[English \(US\)](#) [Español](#) [Français \(France\)](#) [中文\(简体\)](#) [العربية](#) [Português \(Brasil\)](#) [Italiano](#) [한국어](#) [Deutsch](#) [हिन्दी](#) [日本語](#) [+](#)

[Sign Up](#) [Log In](#) [Messenger](#) [Facebook Lite](#) [Video](#) [Meta Pay](#) [Meta Store](#) [Meta Quest](#) [Ray-Ban Meta](#) [Meta AI](#) [Instagram](#) [Threads](#)
[Privacy Policy](#) [Consumer Health Privacy](#) [Privacy Center](#) [About](#) [Create ad](#) [Create Page](#) [Developers](#) [Careers](#) [Cookies](#) [Ad choices](#) [Terms](#)
[Help](#) [Contact](#) [Uploading & Non-Users](#)

Meta © 2026