# CVE Detail – CVE-2025-27363

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.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.98611

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-787: Out-of-bounds Write

## Affected Products

* cpe:2.3:a:freetype:freetype:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:11.0:\*:\*:\*:\*:\*:\*:\*