

CVE-2025-27363

FreeType Out-of-Bounds Write Vulnerability

CISA KEV since May 6, 2025

Actively exploited

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.

EVRS 75_{/100} Urgent priority	CVSS V3.1 8.1 High · NVD	EPSS 0.278 98.1st percentile · FIRST	CISA DEADLINE May 27, 2025 KEV since 2025 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.278 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
freetype	≤ 2.13.0	no fixed version listed	NVD
debian linux	11.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-g8qj-jv5h-78cp

source.android.com source.android.com/docs/security/bulletin/2025-05-01

NVD nvd.nist.gov/vuln/detail/CVE-2025-27363

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-6367

Current data evulnable.com/vulnerability-management/cve/CVE-2025-27363

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.