Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

FreeType Under Attack: Critical Font Parsing Flaw Exposes Millions

Date of Publication	Admiralty Code	TA Number
March 13, 2025	A1	TA2025077

Summary

First Seen: March 2025
Affected Products: FreeType
Affected Platforms: Linux, Android, Windows
Impact: A serious security flaw has been discovered in the widely used FreeType font rendering library, identified as CVE-2025-27363. This out-of-bounds write vulnerability affects FreeType versions 2.13.0 and earlier, occurring when parsing font subglyph structures in TrueType GX and variable font files. If exploited, it could lead to arbitrary code execution, posing a significant risk. Notably, this vulnerability may have been exploited in the wild, making it crucial for users to apply security updates immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-27363	FreeType Out of Bounds Write Vulnerability	FreeType	✗	✓	✓

Vulnerability Details

#1

A high security flaw has been identified in the FreeType font rendering library, a widely used open-source component that powers font rendering across millions of systems. Tracked as CVE-2025-27363, this vulnerability could allow remote attackers to execute arbitrary code, posing a significant risk to users across multiple platforms, including Linux, Android, game engines, GUI frameworks, and various online services. Several Linux distributions are running outdated versions of FreeType, making them susceptible to this vulnerability.

#2 The issue stems from an out-of-bounds write present in FreeType versions 2.13.0 and earlier. It occurs when parsing font subglyph structures in TrueType GX and variable font files, leading to memory corruption. Specifically, a signed short value is incorrectly assigned to an unsigned long, causing a miscalculated buffer size. This flaw allows attackers to write up to six signed long integers beyond the allocated memory, potentially leading to system compromise.

#3 In simpler terms, a maliciously crafted font file could exploit this flaw to manipulate memory, ultimately granting attackers the ability to execute harmful code on vulnerable systems. Given that this vulnerability may have been exploited in the wild, users and administrators are strongly urged to update FreeType to the latest patched version as soon as possible to mitigate potential threats.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-27363	FreeType (FreeType) Version form 0.0.0 through 2.13.0	cpe:2.3:a:freetype:freetype:*:*:*:*:*:*:*:*	CWE-787

Recommendations

Stay Updated: Ensure your FreeType library is upgraded to the latest patched version 2.13.3 and keep all systems, applications, and software relying on FreeType, such as Linux, Android, game engines, and GUI frameworks are fully updated to prevent potential exploitation.

Be Cautious with Fonts: Avoid opening or using untrusted font files, especially those from unknown sources or embedded in web content, to reduce the risk of exploitation.

Enhance Security Measures: Use intrusion detection systems (IDS) and endpoint protection to monitor suspicious activity related to font rendering. Additionally, run applications using FreeType with minimal privileges to reduce the risk of exploitation.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application	

Patch Details

To safeguard against the CVE-2025-27363 vulnerability, update your FreeType library to the latest version 2.13.3.

Link: https://freetype.org/download.html

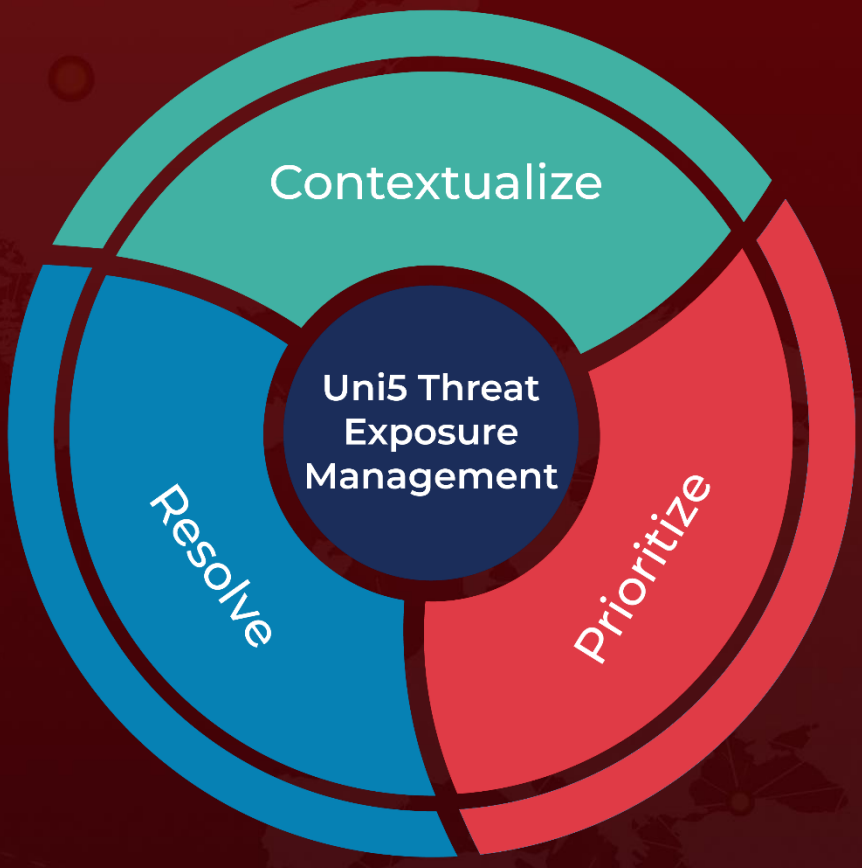
References

https://www.facebook.com/security/advisories/cve-2025-27363

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 13, 2025 • 4:45 AM

More at www.hivepro.com