



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates - Android
Tracking #:432317218
Date:06-05-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Google has released its May 2025 Android security update, addressing a total of 47 vulnerabilities, including an actively exploited high-severity flaw.

TECHNICAL DETAILS:

Google has released its May 2025 Android security update, addressing a total of 47 vulnerabilities, including an actively exploited high-severity flaw, **CVE-2025-27363**, in the FreeType font rendering library.

Originally disclosed by Facebook in March 2025, this vulnerability is currently under limited, targeted exploitation and poses a significant threat due to its potential to enable arbitrary code execution on affected devices.

The update covers critical security issues across various Android components, including the Android Framework, System, and hardware-specific components from Arm, Imagination Technologies, MediaTek, and Qualcomm. Google has provided two patch levels — 2025-05-01 and 2025-05-05 — to allow Android OEMs to deliver fixes in stages.

Given the widespread use of FreeType in billions of devices globally and the potential severity of exploitation, users and enterprise security teams are urged to apply updates immediately and ensure vulnerable systems are patched.

Note: Refer to Android Security Bulletin for additions CVEs and more information

RECOMMENDATIONS:

- Prioritize patch deployment across all Android-based devices especially those used for sensitive operations or with administrative privileges.
- Conduct a risk assessment for any systems running vulnerable versions of FreeType.
- Monitor systems for signs of exploitation, particularly on devices that may be targets of APT groups or espionage campaigns

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://source.android.com/docs/security/bulletin/2025-05-01>