

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Actively Exploited Zero-Days in Android Devices

Tracking #:432318087

Date:03-12-2025

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 released its monthly Android Security bulletin to address multiple security vulnerabilities including two exploited Zero-Days.

TECHNICAL DETAILS:

Google released its monthly Android Security Bulletin addressing 107 security vulnerabilities spanning the Android Framework, System, Kernel, and components from multiple third-party vendors (Arm, Imagination Technologies, MediaTek, Qualcomm, and Unison). Two of the patched vulnerabilities—CVE-2025-48633 and CVE-2025-48572—have been confirmed as exploited in the wild, marking them as high-priority risks for all Android users and enterprise mobility security teams.

Google has disclosed limited information about the nature, attack vector, or actors behind the exploitation, but warns that the vulnerabilities “may be under limited, targeted exploitation.”

Actively Exploited Zero-Day Vulnerabilities

- CVE-2025-48633 – Information disclosure in Framework
- CVE-2025-48572 – Elevation of privilege in Framework

Additional High-Impact Vulnerabilities

- CVE-2025-48631 – Critical Framework Remote DoS

Critical Kernel Elevation-of-Privilege Vulnerabilities

- CVE-2025-48623 – pKVM
- CVE-2025-48624 – IOMMU
- CVE-2025-48637 – pKVM
- CVE-2025-48638 – pKVM

RECOMMENDATIONS:

- Update Immediately: Install the latest security update corresponding to 2025-12-05 patch level
- Avoid Sideloading Apps: Only use apps from Google Play or trusted enterprise sources.
- Enable Google Play Protect: Ensure device scanning is active.

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/2025-12-01>