



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates - Android**  
Tracking #:432317349  
Date:04-06-2025

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 security updates to patch multiple vulnerabilities in the Android OS.

## TECHNICAL DETAILS:

Google has released the June 2025 Android Security Bulletin, addressing multiple high-severity vulnerabilities across Android OS and associated hardware components.

The most critical vulnerability this month is a high-severity escalation of privilege (EoP) flaw in the System component (CVE-2025-26443), which could allow an attacker to gain elevated access on a device with minimal user interaction and no additional execution privileges required.

### Key Vulnerabilities:

#### System Component

- **CVE-2025-26443:** Local privilege escalation flaw in the System component. This is the most severe vulnerability this month, allowing an attacker to gain elevated privileges with minimal user interaction and no additional execution privileges required.

#### Framework Component

- **CVE-2025-26450:** Elevation of privilege vulnerability affecting Android versions 13, 14, and 15.
- **CVE-2025-26455:** Another elevation of privilege vulnerability in the Framework, also impacting Android 13, 14, and 15.

#### Android Runtime

- **CVE-2025-26456:** Denial of Service (DoS) vulnerability in Android Runtime, potentially causing permanent device disruption without user interaction. Affects Android 14 and 15.

#### System Information Disclosure

- **CVE-2025-26441:** Information disclosure vulnerability in the System component, affecting Android 13, 14, and 15.

#### Third-Party Hardware Components

- **Arm (Mali GPU):** CVE-2025-0073 – High-severity issue in Mali GPU drivers.
- **Imagination Technologies (PowerVR GPU):** CVE-2024-12576 – High-severity flaw in PowerVR GPU drivers.
- **Qualcomm Kernel:** CVE-2025-21424 – High-severity kernel vulnerability affecting Qualcomm-powered devices.

**Note:** Refer to the Android Security Bulletin for additional CVEs and more information.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating Android devices to the latest version.

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/2025-06-01>