



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates - Android**  
Tracking #:432317052  
Date:09-04-2025

## 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 critical security updates for Android devices, addressing 62 vulnerabilities, including two actively exploited high-severity flaws and several critical issues. Immediate action is recommended.

### High-Severity Vulnerabilities (Exploited in the Wild):

- **CVE-2024-53150** (CVSS Score: 7.8) - Out-of-bounds flaw in the USB sub-component of Kernel: This vulnerability could lead to information disclosure.
- **CVE-2024-53197** (CVSS Score: 7.8) - Privilege escalation flaw in the USB sub-component of Kernel: This vulnerability could allow an attacker to gain elevated privileges on the device.

### Critical Vulnerabilities:

Google highlighted additional critical vulnerabilities in the System component:

- **CVE-2025-22429**
- **CVE-2025-26416**
- **CVE-2025-22423**
- **CVE-2024-45551**

These flaws could lead to remote privilege escalation without requiring user interaction or additional execution privileges

**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/2025-04-01>