مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Android

Tracking #:432319050

Date:02-06-2026

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 INTELLGIENCE 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 address multiple vulnerabilities in the Android OS.

TECHNICAL DETAILS:

Google has released its June 2026 Android Security Bulletin addressing multiple vulnerabilities affecting Android devices and components, including Framework, System, Kernel, Google Play system modules, and vendor-specific components from Qualcomm, MediaTek, Imagination Technologies, and Unisoc. Several vulnerabilities could allow remote code execution, escalation of privilege, information disclosure, or denial-of-service attacks. Security patch levels **2026-06-01** and **2026-06-05** address these issues.

Vulnerability Details

- **CVE:** Multiple Vulnerabilities (including CVE-2025-65018, CVE-2026-0043, CVE-2026-0097, CVE-2025-47392, CVE-2026-25276, CVE-2025-48595 and others)
- **Severity / CVSS:** Critical / Multiple CVSS Scores
- The June 2026 Android Security Bulletin addresses numerous vulnerabilities across core Android components and third-party chipset/vendor components. The most severe vulnerabilities include remote and local escalation of privilege issues that require no additional execution privileges and, in some cases, no user interaction. The update also resolves multiple denial-of-service, information disclosure, and remote code execution vulnerabilities.
- Successful exploitation of these vulnerabilities may enable attackers to obtain elevated privileges, execute malicious code, disclose sensitive information, disrupt device functionality, or compromise device security. Android indicated that **CVE-2025-48595** may be under limited, targeted exploitation.

Affected Products and Versions

Affected products include Android devices running supported versions with vulnerable components, including:

- Android 14, 15, 16, 16-qpr2
- Devices using affected vendor components from Qualcomm, MediaTek, Unisoc, and Imagination Technologies
- Devices using vulnerable kernel, modem, GPU, display, and closed-source chipset components

Note:

Refer to the Android Security Bulletin – June 2026 for additional CVEs and detailed information regarding affected products, impacted software versions, fixed releases, and recommended mitigation measures.

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/2026/2026-06-01