مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited RCE Vulnerability in Android

Tracking #:432316118

Date:06-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Android released a security bulletin to address multiple vulnerabilities, including a high-severity remote code execution (RCE) exploited in targeted attacks.

TECHNICAL DETAILS:

The August patch addresses a total of 47 flaws, including those identified in components associated with Arm, Imagination Technologies, MediaTek, and Qualcomm.

Other resolved issues include 12 privilege escalation flaws, one information disclosure bug, and one denial-of-service (DoS) flaw impacting the Android Framework.

Notable Vulnerability:

- **CVE-2024-36971** | Base Score: 7.8 – HIGH
  - The zero-day is a use after free (UAF) weakness in the Linux kernel's network route management.
  - It requires System execution privileges for successful exploitation and allows altering the behaviour of certain network connections.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends referring to the security bulletin released by Android and applying the patches as soon as possible.

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/2024-08-01