



مجلس الأمن السيبراني

CYBER SECURITY COUNCIL



Exploited Vulnerability in Android Pixel

Tracking #:432315963

Date:19-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Android Pixel that is being actively exploited by threat actors to gain privilege escalation.

TECHNICAL DETAILS:

Google released an Android Security Bulletin on June 2024, which addressed an exploited vulnerability in pixel devices for potential bypass due to a logic error in the code.

Exploiting this vulnerability could allow for local escalation of privilege without requiring additional execution privileges.

Notable Vulnerability:

- **CVE-2024-32896 | CVSS Score: 7.8 | High | Android Pixel Privilege Escalation Vulnerability** | This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.

All supported Google devices will receive an update to the 2024-06-05 patch level.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Google.

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/security/bulletin/pixel/2024-06-01>