



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – Google Pixel

Tracking #:432315751

Date:04-04-2024

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 recently released security updates to address multiple vulnerabilities in Google Pixel devices.

TECHNICAL DETAILS:

Google announced patches for 25 bugs in Pixel devices, including two issues exploited in the wild in April 2024 Pixel Update Bulletin. Two of the vulnerabilities (**CVE-2024-29745** and **CVE-2024-29748**) are confirmed to be exploited in limited, targeted attacks. Updating Pixel devices to the 2024-04-05 security patch level or later mitigates these vulnerabilities.

A total of 24 vulnerabilities leading to elevation of privilege (EoP) and information disclosure were addressed in various Pixel components, and another was resolved in Qualcomm components.

The most severe of these vulnerabilities is **CVE-2024-29740**, an EoP defect in the System component that affects Android 13 and Android 14.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating Pixel devices to the latest version 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:

1. <https://source.android.com/docs/security/bulletin/pixel/2024-04-01>