مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Qualcomm Chipset Vulnerabilities

Tracking #:432316373

Date:08-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Qualcomm has disclosed multiple vulnerabilities affecting its chipsets including an actively exploited vulnerability.

TECHNICAL DETAILS:

Qualcomm has disclosed multiple vulnerabilities affecting its chipsets. These vulnerabilities pose significant risks, including potential remote code execution and unauthorized access to sensitive data. **CVE-2024-43047**, which affects its Digital Signal Processor (DSP) service and has reportedly been exploited in the wild.

Key Vulnerabilities Identified:

1. **CVE-2024-43047** (CVSS 7.8): The vulnerability has reportedly been exploited in the wild, prompting Qualcomm to issue urgent patches for affected devices.Affects the FASTRPC driver, allowing attackers to exploit memory corruption.
2. **CVE-2024-33066** (CVSS 9.8): Critical flaw in the WLAN Resource Manager enabling remote code execution through improper input validation.
3. **CVE-2024-23369**: High-severity vulnerability in the Hardware Abstraction Layer Operating System (HLOS) allowing local attackers to exploit memory corruption.
4. **CVE-2024-33064**: Buffer over-read flaw in WLAN Host Communication leading to denial of service or information disclosure.

RECOMMENDATIONS:

- Qualcomm has made patches available to Original Equipment Manufacturers (OEMs) and strongly recommends that these updates be deployed promptly on affected devices.
- Users are advised to contact their device manufacturers for specific patch status updates.

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://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html