مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Qualcomm

Tracking #:432316117

Date:06-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Qualcomm released a security bulletin to address multiple vulnerabilities in their products.

TECHNICAL DETAILS:

These vulnerabilities affect Qualcomm closed-source components and are described in further detail in the appropriate Qualcomm security bulletin or security alert. The security rating of these issues is provided directly by Qualcomm.

Vulnerability Details (including but not limited to):

- **CVE-2024-23350** | Security Rating: Critical | CVSS Score: 6.5 - Medium | Reachable Assertion in Multi-Mode Call Processor
  - Permanent DOS when DL NAS transport receives multiple payloads such that one payload contains SOR container whose integrity check has failed, and the other is LPP where UE needs to send status message to network.

- **CVE-2024-21481** | Security Rating: High |CVSS Score: 8.4 - High | Improper Restriction of Operations within the Bounds of a Memory Buffer in Hypervisor
  - Memory corruption when preparing a shared memory notification for a memparcel in Resource Manager.

- **CVE-2024-23356** | Security Rating: High |CVSS Score: 7.8 - High | Improper Restriction of Operations within the Bounds of a Memory Buffer in HLOS
  - Memory corruption during session sign renewal request calls in HLOS.

Note: Patches are being actively shared with OEMs, who have been notified and strongly recommended to deploy those patches on released devices as soon as possible.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates 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://docs.qualcomm.com/product/publicresources/securitybulletin/august-2024-bulletin.html