مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Qualcomm Chipset Vulnerabilities - May 2026 Security Bulletin

Tracking #:432318890

Date:05-05-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Qualcomm Technologies released its May 2026 security bulletin detailing numerous vulnerabilities across its chipsets and associated software components. These affect smartphones, automotive systems, IoT devices, and industrial platforms.

TECHNICAL DETAILS:

Qualcomm Technologies has disclosed a broad set of critical and high-severity vulnerabilities in its May 2026 security bulletin. These flaws impact a wide spectrum of devices, including smartphones, automotive systems, and industrial IoT platforms.
Several vulnerabilities—most notably CVE-2026-25254 (CVSS 9.8)—enable remote code execution (RCE) without user interaction, significantly elevating risk. Others allow local privilege escalation, firmware compromise, and denial-of-service (DoS) conditions.

Critical Severity Vulnerabilities

- CVE-2026-25254 (CVSS: 9.8): Improper authorization in the Qualcomm Software Center, specifically the SocketIO interface. Allows unauthenticated remote attackers to execute arbitrary code and gain complete control over the application environment.
- CVE-2026-25293 (CVSS: 9.6): Buffer overflow due to incorrect authorization checks in the powerline communication (PLC) firmware. Enables adjacent network attackers to execute malicious payloads.
- CVE-2026-25262 (CVSS: 6.9): Write-what-where memory corruption in the Primary Bootloader when processing a maliciously crafted ELF file. Requires local or physical access but allows bypassing secure boot and establishing deep firmware-level persistence.

High Severity Vulnerabilities

- CVE-2026-25255 (CVSS: 8.8): Exposed dangerous function in the Qualcomm Package Manager and Software Center via the gRPC server interface, enabling privilege escalation.
- CVE-2026-24082 (CVSS: 7.8): Use-after-free vulnerability in Automotive GPU components. Occurs during performance counter deselect operations when copying data from a freed source, potentially destabilizing vehicle infotainment or telemetry systems.
- CVE-2025-47408 (CVSS: 7.8): Untrusted pointer dereference in WINBLAST-POWER firmware. Allows memory corruption via IOCTL calls with invalid buffers from a driver.
- CVE-2025-47401 (CVSS: 6.5): Buffer over-read in WLAN HAL during channel configuration (target power rate tables), causing transient denial of service.
- CVE-2025-47403 (CVSS: 6.5): Buffer over-read in WLAN Firmware when processing malformed fast transition response frames during wireless roaming, causing transient DoS.

RECOMMENDATIONS:

- Inventory all Qualcomm-based devices and apply available security updates as soon as they are released by the device vendor.

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/securitybulletin/may-2026-bulletin.html