مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Samsung Mobile

Tracking #:432318738

Date:07-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Samsung Mobile has released security updates for its major flagship models to address multiple vulnerabilities.

TECHNICAL DETAILS:

Samsung has released the April 2026 Security Maintenance Release (SMR) addressing multiple vulnerabilities affecting Samsung Galaxy devices. The update includes patches from the Android Security Bulletin, Samsung Semiconductor, and Samsung-specific components. The vulnerabilities range from critical to moderate severity and could allow remote code execution, privilege escalation, sensitive data exposure, and security feature bypass under certain conditions.

Vulnerability Details:
Google Android Vulnerabilities:
Critical
CVE-2023-20713, CVE-2025-47392, CVE-2025-64505, CVE-2025-64720, CVE-2025-65018, CVE-2026-0039, CVE-2026-0040, CVE-2026-0041, CVE-2026-0042, CVE-2026-0043, CVE-2026-0044, CVE-2026-0049, CVE-2026-0052, CVE-2026-0080

High
CVE-2025-22424, CVE-2025-22426, CVE-2025-48600, CVE-2025-48651(A-467762899), CVE-2026-0016, CVE-2026-0018, CVE-2026-0036, CVE-2026-0045, CVE-2026-0046, CVE-2026-0048, CVE-2026-0050, CVE-2026-0055, CVE-2026-0056, CVE-2026-0058, CVE-2026-0059, CVE-2026-0067, CVE-2026-0079, CVE-2026-21381

Moderate
CVE-2026-20435

Samsung Semiconductor:
High
CVE-2025-52908, CVE-2025-52909, CVE-2025-54601, CVE-2025-54602

Samsung Vulnerabilities and Exposures (SVE)
High Severity

- **SVE-2025-2188 (CVE-2026-21007)**
  Improper validation in Device Care allows Knox Guard bypass (physical attack).
- **SVE-2025-2589 (CVE-2026-21010)**
  Improper input validation in Retail Mode allows unauthorized privileged operations.
- **SVE-2026-0775 (CVE-2026-21003)**
  Weak validation enables bypass of network restrictions.

Moderate Severity

- **SVE-2025-1863 (CVE-2026-21006)**
  Improper access control in Samsung DeX exposes hidden notifications.
- **SVE-2025-2300 (CVE-2026-21008)**
  Sensitive information exposure in S Share.
- **SVE-2025-2443 (CVE-2026-21009)**
  Improper checks allow App Pinning bypass via Recents UI.

- **SVE-2026-0025 (CVE-2026-21012)**
  Improper file handling in AOD Manager allows privileged file creation.
- **SVE-2026-0102 (CVE-2026-21011)**
  Incorrect Bluetooth privilege assignment allows Extend Unlock bypass.

Affected Products

- Samsung Galaxy devices running:
  - **Android 14**
  - **Android 15**
  - **Android 16**

RECOMMENDATIONS:

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

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://security.samsungmobile.com/securityUpdate.smsb