مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Samsung Mobile

Tracking #:432318343

Date:03-02-2026

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 Mobile has released its February 2026 Security Maintenance Release (SMR-FEB-2026) for major flagship devices as part of its monthly security update process. This release includes security patches from both Google (Android Security Bulletin) and Samsung, addressing multiple high-severity vulnerabilities that could impact the confidentiality, integrity, and stability of affected devices.

Vulnerability Details:

Google Android Vulnerabilities

The February 2026 SMR includes fixes for the following high-severity CVEs from the Android Security Bulletin:

High-Severity CVEs:

CVE-2025-47366, CVE-2025-47397, CVE-2025-47398, CVE-2025-47402, CVE-2025-48630, CVE-2025-48641, CVE-2025-48645, CVE-2025-48646, CVE-2025-48649, CVE-2025-48650, CVE-2026-0014, CVE-2026-0015, CVE-2026-0017, CVE-2026-0018, CVE-2026-0020, CVE-2026-0021, CVE-2026-0023, CVE-2026-20401, CVE-2026-20403, CVE-2026-20404, CVE-2026-20405, CVE-2026-20406, CVE-2026-20420, CVE-2026-20421, CVE-2026-20422

Samsung Vulnerabilities and Exposures (SVE)

Samsung Mobile addressed 7 Samsung-specific vulnerabilities.

High Severity

- **SVE-2025-1140 (CVE-2026-20977)**
  Improper access control in *Emergency Sharing* could allow local attackers to disrupt its functionality.
- **SVE-2025-1217 (CVE-2026-20983)**
  Improperly exported components in *Samsung Dialer* could allow local attackers to launch arbitrary activities with elevated privileges.
- **SVE-2025-2226 (CVE-2026-20978)**
  Improper authorization in *KnoxGuardManager* could allow bypass of application persistence configuration.
- **SVE-2025-2289 (CVE-2026-20979)**
  Improper privilege management in *Settings* could allow launching arbitrary activities with system privileges.
- **SVE-2025-2473 (CVE-2026-20980)**
  Improper input validation in *PACM* could allow a physical attacker to execute arbitrary commands.

Moderate Severity

- **SVE-2025-2705 (CVE-2026-20981)**
  Improper input validation in *FacAtFunction* could allow a privileged physical attacker to execute commands with system privileges.
- **SVE-2025-2706 (CVE-2026-20982)**
  A path traversal issue in *ShortcutService* could allow privileged local attackers to create files with system privileges.

Affected Versions

- Samsung Mobile devices running Android 13, 14, 15, and 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