مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Samsung Mobile

Tracking #:432317783

Date:07-10-2025

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 its October 2025 Security Maintenance Release (SMR-OCT-2025), which delivers critical security improvements for Samsung mobile devices. This monthly security package includes fixes from the Google Android Security Bulletin – October 2025 as well as Samsung Vulnerabilities and Exposures (SVE) updates.

Google Patches

- **High Severity:** CVE-2025-22420, CVE-2025-32328, CVE-2025-32329, CVE-2025-48570, CVE-2025-48572, CVE-2025-48573, CVE-2025-48580, CVE-2025-48591, CVE-2025-48584, CVE-2025-48536, CVE-2025-48555, CVE-2025-48607, CVE-2025-47354, CVE-2025-47351

Samsung Vulnerabilities & Exposures (SVE)

In addition to Google patches, **20 Samsung-specific vulnerabilities** are addressed. Key fixes include:

- **Fingerprint Trustlet SVE-2024-1838(CVE-2025-21044)** – High – Out-of-bounds write enabling privileged attackers to write memory.
- **Galaxy Watch SVE-2025-0021(CVE-2025-21045)** – Moderate – Insecure storage of sensitive information.
- **Samsung DeX SVE-2025-0465(CVE-2025-21046)** – Moderate – Improper access control exposing recent app list.
- **Contacts SVE-2025-0903(CVE-2025-21050)** – High – Input validation flaw allowing cross-user data access.
- **KnoxGuard SVE-2025-1503(CVE-2025-21047)** – Moderate – Privileged API misuse through improper access control.
- **Knox Enterprise SVE-2025-1526(CVE-2025-21048)** – High – Path traversal leading to arbitrary code execution.
- **Image Processing Libraries (SVE-2025-1527, SVE-2025-1528, SVE-2025-1529, SVE-2025-1540)** – Moderate – Multiple out-of-bounds memory issues in **libpadm.so** JPEG decoding.
- **SecSettings SVE-2025-1620(CVE-2025-21049)** – Moderate – Improper access control exposing sensitive settings.
- **libimagecodec.quram.so SVE-2025-1845(CVE-2025-21055)** – High – Out-of-bounds read/write allowing potential remote memory access.

Impact

Exploitation of these vulnerabilities could allow:

- Privilege Escalation (SYSTEM-level access)
- Sensitive Data Exposure across profiles and applications
- Arbitrary Code Execution via path traversal or image decoding flaws
- Information Disclosure through insecure storage and improper access control

Affected Products

- Samsung flagship mobile devices (Android 13–16, Android Watch 14)

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