مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Samsung Mobile

Tracking #:432317705

Date:15-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

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 September 2025 Security Maintenance Release (SMR-SEP-2025) for flagship devices. This update integrates security patches from Google Android Security Bulletin (September 2025), Samsung Semiconductor, and 25 Samsung-specific vulnerability fixes (SVE).

The release resolves several critical and high-severity vulnerabilities, including a remote code execution vulnerability (CVE-2025-21043) in libimagecodec.quram.so that has been confirmed to be actively exploited in the wild. Organizations and end-users are strongly advised to apply this update immediately.

Vulnerability Details
Google Security Patches
Samsung integrated multiple fixes from the **Android Security Bulletin – September 2025**, including:

- **Critical**
  - CVE-2025-48539
  - CVE-2025-27034
- **High**
  Multiple vulnerabilities including CVE-2025-48543, CVE-2025-0089, CVE-2025-48540, CVE-2025-48546, CVE-2025-48548, CVE-2025-48549, CVE-2025-48552, CVE-2025-48553, CVE-2025-48556, CVE-2025-48558, CVE-2025-48563, CVE-2025-48537, CVE-2025-48545, CVE-2025-48560, CVE-2025-48561, CVE-2025-48562, CVE-2025-48538, CVE-2025-48542, CVE-2025-48550, CVE-2025-48554, CVE-2025-48559, CVE-2023-40130, CVE-2025-26464, CVE-2025-32323, CVE-2025-32327, CVE-2025-48532, CVE-2025-48535, CVE-2025-48541, CVE-2025-48544, CVE-2025-48547, CVE-2025-48581, CVE-2025-26447, CVE-2025-48551, CVE-2025-48524, CVE-2025-48534, CVE-2024-7881, CVE-2024-47898, CVE-2024-47899, CVE-2025-0467, CVE-2025-46710, CVE-2025-25179, CVE-2025-25180, CVE-2025-8109, CVE-2025-1706, CVE-2025-21701, CVE-2025-21756, CVE-2025-1246, CVE-2025-46708, CVE-2025-46707, CVE-2025-38352, CVE-2025-27032, CVE-2025-21482, CVE-2025-47326, CVE-2025-47329, CVE-2025-47328, CVE-2025-20708, CVE-2025-20703, CVE-2025-3212

Samsung Semiconductor Patch

- **High**: CVE-2025-32100

Samsung Vulnerabilities and Exposures (SVE)
Samsung addressed **25 SVE items** in this release. Highlights include:

- **SVE-2024-2288 (CVE-2025-21032)** – Improper access control in One UI Home
- **SVE-2025-0012 (CVE-2025-21033)** – Improper access control in ContactProvider
- **SVE-2025-0633 (CVE-2025-21025)** – Improper access control in MARsExemptionManager
- **SVE-2025-0659 (CVE-2025-21034)** – Out-of-bounds write in libsavsvc.so (High)
- **SVE-2025-0693 (CVE-2025-21026)** – Improper permission handling in ImsService

- **SVE-2025-0697 (CVE-2025-21027)** – Improper intent verification in ImsService
- **SVE-2025-0954 (CVE-2025-21028)** – Improper privilege management in ThemeManager
- **SVE-2025-0980 (CVE-2025-21029)** – Improper permission handling in System UI
- **SVE-2025-1016 (CVE-2025-21030)** – Improper permission handling in AppPrelaunchManagerService
- **SVE-2025-1203 (CVE-2025-21031)** – Improper access control in ImsService
- **SVE-2025-1702 (CVE-2025-21043) – Critical** Out-of-bounds Write in libimagecodec.quram.so
    - Exploit observed in the wild.
    - Allows remote attackers to execute arbitrary code.

Affected Versions

- Samsung flagship models 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