مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - SAMSUNG

Tracking #:432317462

Date:08-07-2025

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 released a security bulletin addressing multiple vulnerabilities, including one critical and 21 high-severity issues linked to Android's July security package, as well as 17 additional vulnerabilities and high-severity exposures affecting its own chipsets.

TECHNICAL DETAILS:

Vulnerability Details:

Android

- **Critical:** CVE-2025-21450
- **High:** CVE-2024-53010, CVE-2025-0819, CVE-2025-26433, CVE-2025-26454, CVE-2025-32321, CVE-2025-22436, CVE-2023-24023, CVE-2024-49714, CVE-2025-32325, CVE-2025-32326, CVE-2025-32331, CVE-2025-32330, CVE-2025-21449, CVE-2025-21446, CVE-2025-21433, CVE-2025-27052, CVE-2025-27057, CVE-2025-27042, CVE-2025-27056, CVE-2025-27043, CVE-2025-27061

Samsung

- **SVE-2024-2304(CVE-2025-20983, CVE-2025-20982): Out-of-bounds write in KnoxVault trustlet |** Severity: High
  - **Affected versions:** Android 14, 15
  - **Reported on:** December 8, 2024
  - **Disclosure status:** Privately disclosed
  - Out-of-bounds write in KnoxVault trustlet prior to SMR Jul-2025 Release 1 allows local privileged attackers to write out-of-bounds memory.
  - The patch adds proper input validation.

- **SVE-2024-2335(CVE-2025-21004): Improper verification of intent by broadcast receiver in SystemUI for Galaxy Watch |** Severity: Moderate
  - **Affected versions**: Android Watch 14
  - **Reported on**: December 12, 2024
  - **Disclosure status**: Privately disclosed
  - Improper verification of intent by broadcast receiver in SystemUI for Galaxy Watch prior to SMR Jul-2025 Release 1 allows local attackers to power off the device.
  - The patch adds access control.

- **SVE-2025-0047(CVE-2025-20997): Incorrect default permission in Framework for Galaxy Watch |** Severity: Moderate
  - **Affected versions:** Android Watch 14
  - **Reported on**: January 9, 2025
  - **Disclosure status**: Privately disclosed
  - Incorrect default permission in Framework for Galaxy Watch prior to SMR Jul-2025 Release 1 allows local attackers to reset some configuration of Galaxy Watch.
  - The patch removes unused code.

- **SVE-2025-0123(CVE-2025-20998): Improper access control in SamsungAccount for Galaxy Watch |** Severity: Moderate
  - **Affected versions:** Android Watch 14
  - **Reported on**: January 22, 2025
  - **Disclosure status**: Privately disclosed
  - Improper access control in SamsungAccount for Galaxy Watch prior to SMR Jul-2025 Release 1 allows local attackers to access phone numbers. The patch adds proper access control.

RECOMMENDATIONS:

The UAE Cyber Security council recommends applying the necessary patches released by Samsung at the earliest.

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