

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates – Samsung Mobile**  
Tracking #:432317049  
Date:08-04-2025

## 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 Mobile has released its Security Maintenance Release (SMR) for April 2025, addressing multiple vulnerabilities across its flagship models. This update includes security patches from Google and Samsung, as well as fixes for Samsung Vulnerabilities and Exposures (SVE).

### 1. Google Patches:

- Includes fixes for vulnerabilities listed in the Android Security Bulletin – April 2025.
- Addresses critical, high, and moderate severity issues, with notable fixes for CVE-2025-22429, CVE-2025-26416, CVE-2025-22423, and CVE-2024-45551

### 2. Samsung Semiconductor Patches:

- Resolves CVE-2025-22377 (High severity), improving security in Samsung Semiconductor products.

### 3. Samsung Vulnerabilities and Exposures (SVE):

- 21 SVE items have been addressed, including critical vulnerabilities such as SVE-2024-1795 (CVE-2025-20936) and high-severity issues like SVE-2024-1695 (CVE-2025-20935).
- Vulnerabilities impact components such as Sticker Center, ClipboardService, HDCP trustlet, Galaxy Watch, and others.

## Critical Vulnerabilities

### SVE-2024-1795 (CVE-2025-20936)

- **Description:** Improper access control in HDCP trustlet allows local attackers with shell privileges to escalate their privileges to root.

### CVE-2025-22429

- **Description:** Exploitable vulnerability in Android framework that could allow remote code execution.

## High-Severity Vulnerabilities

### SVE-2024-1695 (CVE-2025-20935)

- **Description:** Improper handling of insufficient permissions in ClipboardService allows local attackers to access files with system privileges.

### CVE-2025-22377

- **Description:** Vulnerability in Samsung Semiconductor products that could lead to privilege escalation or data exposure.

## Moderate-Severity Vulnerabilities

Several moderate vulnerabilities were addressed, including improper access control issues in SamsungContacts (SVE-2024-1920), InputManager (SVE-2024-2403), and Galaxy Watch Bluetooth pairing (SVE-2025-0255).

## 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>