مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Samsung Mobile

Tracking #:432318903

Date:06-05-2026

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 has released its May 2026 Security Maintenance Release (SMR) for major flagship Galaxy devices, delivering critical Android and Samsung-specific security patches. This update incorporates Google's May 2026 Android Security Bulletin fixes, including critical vulnerabilities, alongside Samsung Vulnerabilities and Exposures (SVE) patches addressing multiple privilege escalation, arbitrary code execution, and sensitive information disclosure issues affecting Galaxy smartphones and Galaxy Watch devices.

Vulnerability Details
Google Android Security Bulletin Patches Included

Critical

- CVE-2026-0051, CVE-2026-0073

High Severity

- CVE-2025-32348, CVE-2025-47401, CVE-2025-47403, CVE-2025-48570, CVE-2025-48615, CVE-2025-48652, CVE-2026-0061, CVE-2026-0062, CVE-2026-0063, CVE-2026-0065, CVE-2026-0069, CVE-2026-0070, CVE-2026-0074, CVE-2026-0075, CVE-2026-0076, CVE-2026-0077, CVE-2026-0078, CVE-2026-0085, CVE-2026-0086, CVE-2026-0087, CVE-2026-0088, CVE-2026-0089, CVE-2026-20447, CVE-2026-20448, CVE-2026-20449, CVE-2026-20450, CVE-2026-24085

Samsung Vulnerabilities and Exposures (SVE)

- **SVE-2026-0483 (CVE-2026-21019)** — High | Arbitrary Code Execution
  Improper input validation in FacAtFunction on Galaxy Watch devices may allow local attackers to execute arbitrary code with system privileges.
- **SVE-2025-2186 (CVE-2026-21021)** — Moderate | Privileged Activity Launch
  Improper input validation in Routines may allow physical attackers to launch privileged activities.
- **SVE-2026-0086 (CVE-2026-21015)** — Moderate | Information Disclosure
  Incorrect default permissions in FactoryCamera may allow unauthorized access to device unique identifiers.
- **SVE-2026-0230 (CVE-2026-21016)** — Moderate | Sensitive Information Disclosure
  Incorrect privilege assignment in LocationManager may allow local attackers to access sensitive information.
- **SVE-2026-0252 (CVE-2026-21022)** — Moderate | Sensitive Information Disclosure
  Insufficient permission handling in Routines may allow unauthorized access to sensitive data.
- **SVE-2026-0478 (CVE-2026-21018)** — Moderate | Arbitrary Code Execution
  Out-of-bounds write in SveService may allow local privileged attackers to execute arbitrary code.
- **SVE-2026-0623 (CVE-2026-21020)** — Moderate | Privileged Function Abuse
  Improper export of Android application components in OmaCP may allow local attackers to trigger privileged functions.

Impact

Successful exploitation of these vulnerabilities could allow attackers to:

- Execute arbitrary code with elevated or system privileges
- Access sensitive user or device information
- Launch unauthorized privileged activities
- Abuse exported system components
- Compromise Galaxy Watch and Galaxy smartphone security

Affected Products

- Samsung devices running Android 14, 15, and 16
- Galaxy Watch devices running Android Watch 14 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