مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical 0-Click Vulnerability in Samsung Devices

Tracking #:432316735

Date:13-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in Samsung smartphones, potentially allowing remote code execution through zero-click attacks.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2024-49415) has been discovered in Samsung smartphones, potentially allowing remote code execution through zero-click attacks. The flaw, which affects devices running Android 12, 13, and 14, has been patched in Samsung's December 2024 security update.

Key Details

- **CVE ID: CVE-2024-49415**
- Severity: Critical rated by Samsung
- Affected Components: Monkey's Audio (APE) decoder, specifically the libsaped.so library
- Impacted Devices: Samsung Galaxy S23, S24, and potentially other models
- Vulnerability Type: Out-of-bounds write

The vulnerability stems from an out-of-bounds write issue in the saped_rec function within the libsaped.so library. This function writes to a DMA buffer allocated by the C2 media service, which has a fixed size of 0x120000 bytes. However, specially crafted APE files with large blocksperframe sizes can cause substantial buffer overflow.

Exploitation Scenario:

The vulnerability is especially concerning because it can be triggered remotely via Rich Communication Services (RCS) messaging, which is enabled by default on Samsung S24 devices. This allows attackers to exploit the vulnerability without any user interaction, increasing the likelihood of successful exploitation.

Affected Versions:

- Samsung S24 (all models and versions)
- Samsung S23 and other Samsung models (potentially affected)

RECOMMENDATIONS:

- Apply the December 2024 Samsung security update immediately.
- Ensure that automatic updates are enabled on devices to receive future patches promptly.
- Consider temporarily disabling RCS on Google Messages until the update is applied.

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