



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- Samsung
Tracking #:432316222
Date:04-09-2024

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 INTELLIGENCE 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 (SMRs) for its major flagship models to address multiple vulnerabilities.

TECHNICAL DETAILS:

Samsung Mobile has released security updates for its major flagship models as part of its monthly Security Maintenance Release (SMR) process. This SMR package includes patches from Google and Samsung, addressing critical and high-severity vulnerabilities.

Google Patches:

The SMR package includes Google patches up to the Android Security Bulletin - September 2024. This bulletin addresses the following CVE items:

Critical-Severity Vulnerability:

CVE-2024-23350

High-Severity Vulnerabilities:

CVE-2024-23355, CVE-2024-21481, CVE-2024-23356, CVE-2024-23357, CVE-2024-33027, CVE-2024-21478, CVE-2024-23383, CVE-2024-23384, CVE-2024-23382, CVE-2024-23381, CVE-2024-23352, CVE-2024-23353, CVE-2024-20082, CVE-2024-33013, CVE-2024-33025, CVE-2024-33015, CVE-2024-33024, CVE-2024-33010, CVE-2024-33020, CVE-2024-33018, CVE-2024-33019, CVE-2024-33026, CVE-2024-2937, CVE-2024-31333, CVE-2024-33011, CVE-2024-33012, CVE-2024-33014, CVE-2024-33023, CVE-2024-4607, CVE-2024-32896, CVE-2024-40658, CVE-2024-40662, CVE-2024-40650, CVE-2024-40652, CVE-2024-40654, CVE-2024-40655, CVE-2024-40657, CVE-2024-40656, CVE-2024-40659, CVE-2024-40665, CVE-2024-40664, CVE-2024-40663, CVE-2024-40666

Samsung Vulnerabilities and Exposures (SVEs):

In addition to Google patches, Samsung Mobile is addressing 23 Samsung Vulnerabilities and Exposures (SVEs). These SVEs cover a range of security issues, including:

- Improper access controls
- Authorization vulnerabilities
- Path traversal issues
- Incorrect use of privileged APIs

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>