MDM Monthly: March 2025

Executive brief | TJ Singh | Published April 5, 2025

Executive Summary

- Microsoft's March Patch Tuesday fixed six exploited zero-days, most of them triggered by mounting a crafted virtual disk, plugging in a USB drive or opening a crafted file.
- Apple's iOS 18.3.2 fixed an exploited WebKit flaw, CVE-2025-24201, and Google's March bulletin lists two Android flaws with limited, targeted exploitation.
- Intune added automatic Apple software update policies and a Samsung Knox partnership, and Jamf Pro 11.15 introduced Blueprints for declarative configuration.

Executive view: cost and risk

- **Opex:** Declarative update policies replace per-OS manual policy edits, which saves recurring labor, but the move needs a pilot and a user-experience decision. Blocking virtual disk mounting and tightening USB controls are policy changes that need testing.
- **Capex:** Samsung Galaxy devices gain hardware-backed attestation, which favors Samsung in a refresh when you need device integrity checks. No other capital item this month.
- **Enterprise impact:** Six exploited Windows flaws in one month, several reachable through a file a user opens or mounts, show that user behavior remains part of the attack path. A WebKit sandbox escape on iPhones used against targeted individuals puts high-risk roles first.
- **Decision needed:** Approve a plan to move Apple update enforcement to declarative policies, and decide whether virtual disk mounting is blocked for standard users.

My position

Move Apple software updates to declarative management now, because Intune and Jamf both ship the tools and the legacy commands have no future.

I'm TJ Singh, a managing principal in mobility and endpoint management with more than 20 years of global experience in the device management field.
Full issue: https://www.tjsinghsahota.com/mdm-monthly-march-2025/
AI tools may have been used to conduct research for this article.