MDM Monthly: August 2025

Executive brief | TJ Singh | Published September 6, 2025

Executive Summary

- Intune's August release put Multi Admin Approval on the Wipe action and on role and permission changes, so one stolen admin credential no longer wipes devices alone.
- Apple fixed an exploited ImageIO flaw, CVE-2025-43300, on August 20, and says it may have been used in an extremely sophisticated attack against specific targeted individuals.
- Microsoft's August Patch Tuesday fixed 107 CVEs and one publicly disclosed Kerberos flaw, and Android's August bulletin carries fixes for two Qualcomm flaws that Qualcomm had earlier flagged as possibly under limited, targeted exploitation.

Executive view: cost and risk

- **Opex:** Second-admin approval adds a few minutes to each wipe and an approver rota. Measuring time-to-patch for exploited flaws costs reporting work once, then runs on its own. Platform SSO on macOS going generally available means a project for Mac fleets still using older sign-in flows.
- **Capex:** Ubuntu 20.04 devices can no longer enroll new in Intune, so Linux fleets on that release are an upgrade item. No other hardware spend is driven by this month.
- **Enterprise impact:** A flaw Apple says may have been exploited against targeted individuals puts executives and other high-risk roles first. A stolen UEM admin credential that can wipe devices without a second approver puts the whole fleet at risk.
- **Decision needed:** Turn on Multi Admin Approval for Wipe and for role changes. Agree a target number of days for exploited-flaw patches and start reporting it.

My position

Track how long exploited flaws stay open on your fleet, and put a second approver in front of wipe.

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-august-2025/
AI tools may have been used to conduct research for this article.