MDM Monthly: May 2025

Executive brief | TJ Singh | Published June 7, 2025

Executive Summary

- Ivanti disclosed two flaws in Endpoint Manager Mobile on May 13, CVE-2025-4427 and CVE-2025-4428, that chain into unauthenticated remote code execution and were exploited in the wild to a limited degree.
- Microsoft's May Patch Tuesday fixed five exploited Windows flaws, and Google's May bulletin lists a FreeType flaw, CVE-2025-27363, with limited, targeted exploitation.
- Intune's May release marks rooted corporate Android devices noncompliant automatically and adds an Endpoint Privilege Management Deny rule.

Executive view: cost and risk

- **Opex:** An emergency patch for a management server means an out-of-cycle change window, a backup and a rollback plan. Searching HTTP logs for the exploited endpoints and filtering API access are extra hours when the alert lands.
- **Capex:** Self-hosted MDM carries hosting, patching and monitoring costs that a cloud service moves to the vendor, so compare the two at your next renewal. DigiCert is retiring its legacy Managed PKI in October 2025, which affects certificate issuance for Jamf customers using it.
- **Enterprise impact:** An MDM server can push configuration, apps and commands to every managed device, so a remote code execution flaw on it is a fleet-wide risk. CISA listing both flaws as exploited sets the clock for everyone.
- **Decision needed:** Decide whether the on-premises MDM server stays on premises, and agree a maximum number of days from an exploited-flaw advisory to a patched server.

My position

Treat an on-premises MDM server as internet-facing infrastructure that gets patched in days, not in the monthly cycle.

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