Patch Management Awareness Guide

Unpatched systems are low-hanging fruit for attackers. Known vulnerabilities with available patches are actively exploited, often within hours of disclosure. A disciplined patch management process is one of the most impactful security controls you can implement.

Key Points

- ✓ Patch critical vulnerabilities within 24-48 hours of release
- ✓ Prioritize based on CVSS score, exploitability, and asset criticality
- ✓ Test patches in a staging environment before deploying to production
- ✓ Maintain an accurate inventory of all systems and software versions
- ✓ Automate patching where possible — WSUS, SCCM, Intune, Ansible
- ✓ Track patch compliance metrics and report to leadership monthly
- ✓ Have a rollback plan for every patch deployment

Action Items

1. Enable automatic updates on all workstations and personal devices
2. Subscribe to vendor security advisory mailing lists (Microsoft, Adobe, etc.)
3. Review your organization's patch compliance dashboard this week
4. Identify any systems running end-of-life software and plan upgrades

Quick Reference

Patch Priority Matrix:
Critical + Internet-facing + Exploit available = Patch within 24 hours
High + Internal + No exploit = Patch within 7 days
Medium + Low risk = Patch within 30 days
Low + No exposure = Next maintenance window
Common Vulnerability Sources: NVD (nvd.nist.gov), CVE (cve.org), vendor advisories, CISA KEV catalog