

Known Flaws, Open Doors: Why Patch Management Matters

A durable program for finding, fixing, and reporting known vulnerabilities.



Software vulnerabilities are a predictable path into the network. When patches are delayed, missed, or poorly tracked, known weaknesses can remain exposed long after fixes are available. A durable patch-management program gives executives evidence that vulnerabilities are being identified, prioritized, remediated in a timely fashion, and reported—not merely assumed to be under control.

What an Effective Program Should Include



Accurate asset inventory

Maintain a current inventory of hardware, software, cloud services, appliances, and supported versions, with accountable owners.



Remove unsupported software

Many software manufacturers do not include automated removal of previous software versions which means patch automation software can leave them behind. Use asset and scanning tools to surface outdated software and remove manually if necessary.



AI-assisted analysis

Use an approved AI tool to compare inventories, scan results, vendor notices, and patch reports; surface gaps; and assist with remediation prioritization. Keep people accountable for validation and final risk decisions.



Remediation discipline

Define risk-based deadlines, testing and deployment procedures, exception approvals, compensating controls, escalation paths, and verification of closure.



Internal and external scanning

Scan from both perspectives to identify missing patches, exposed services, configuration weaknesses, and assets that internal tools may not see.



Reporting and reconciliation

Compare automated patching reports against the asset inventory. Missing devices, unsupported systems, failed deployments, and exceptions can reveal blind spots in patching coverage.



Vendor vulnerability alerts

Subscribe to alerts from critical technology vendors and ensure advisories are reviewed, assigned, and tracked promptly.



Board-level reporting

Report material exposures, overdue remediation, exceptions, trends, and progress in clear business terms.



Next Steps

Ask IT or internal audit to confirm that the credit union has a **durable patch-management, reporting, and remediation plan**. Require defined ownership, a regular reporting cadence, documented findings and exceptions, risk-based remediation targets, and evidence that fixes were completed timely. Management should review unresolved gaps, while the board receives a concise view of significant exposure, trends, and accountability.