Vulnerability Remediation Plan

Author: Alexander T. Ramos
Date: October 05, 2025

Purpose

This document outlines the remediation actions and priorities for the vulnerabilities identified during the network and host scan. The goal is to mitigate exploitable risks and strengthen the organization's overall security posture.

Remediation Priorities

Priority	Description	Target Completion
P1 – Critical	Patches or configurations addressing active exploits or unauthenticated access.	Within 24–48 hours
P2 – High	Patches for vulnerabilities that could lead to privilege escalation or lateral movement.	Within 7 days
P3 – Medium	Mitigations for vulnerabilities that require local access or social engineering.	Within 14–30 days
P4 – Low	Cosmetic or low-risk configuration improvements.	Within 60 days

Recommended Actions

■ **Critical**
- SMB Signing Disabled (CVE-2017-0144): Disable SMBv1 via Group Policy, enforce SMB signing, and validate through follow-up scan.

■ **High**
- Apache HTTPD Path Traversal (CVE-2021-41773): Update Apache to v2.4.52 or higher, implement path restrictions, and test after patching.

■ **Medium**
- Weak TLS Cipher Suites: Update web server configuration to allow only TLS 1.2/1.3 and remove deprecated ciphers.

■ **Low**
- Missing Security Headers: Add security headers (`X-Frame-Options`, `X-Content-Type-Options`, `Content-Security-Policy`) and validate via browser dev tools.

Verification Steps

1. Perform follow-up vulnerability scan to confirm remediation.
2. Document patch evidence and validate system hardening.
3. Review logs for failed patch or unauthorized changes.
4. Update vulnerability management dashboard after confirmation.

Lessons Learned

• Establish automated monthly scans.
• Integrate patch management with change control.
• Communicate remediation timelines to system owners.

Prepared by: Alexander T. Ramos – Cybersecurity Analyst