Develop and Apply Risk Management Strategies

Critical (10.0)	43063	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)
Critical (10.0)	44422	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)

- Critical Risk 1: MS09-071
    - Identification of Risks from Vulnerability Scan Results:
        - This vulnerability in the Internet Authentication Service could allow remote code execution. If exploited, it could enable an attacker to execute malicious commands on a vulnerable system without user interaction.
        - Impact: Unauthorized access, data breach, system compromise, or full control of affected systems.
    - Treatment Recommendations and Mitigation Steps:
        - *Recommendation:* Apply Microsoft's security patch (KB974318) immediately.
        - *Basic Mitigation Steps:*
            1. Verify affected systems using Microsoft's advisory details.
            2. Test and deploy the patch in a controlled environment before rolling it out across the network.
            3. Enable firewall rules to block unnecessary network traffic to Internet Authentication Service ports.

- Critical Risk 2: MS10-012
    - Identification of Risks from Vulnerability Scan Results:
        - This vulnerability in the Server Message Block (SMB) protocol could also allow remote code execution. Attackers could exploit this by sending specially crafted requests to vulnerable systems.
        - *Impact:* Network-wide compromise, unauthorized access, potential for ransomware deployment, or destruction of data.
    - Treatment Recommendations and Mitigation Steps:
        - *Recommendation:* Apply Microsoft's security patch (KB971468) immediately.
        - *Basic Mitigation Steps:*
            1. Disable SMBv1 and configure SMB signing where applicable.
            2. Restrict access to SMB ports (e.g., 445) using firewalls.
            3. Regularly update and scan systems for unauthorized configurations.

- Risk Monitoring Procedure:
    - Continuous Risk Monitoring Framework for Vulnerability Management *Procedure:*

1. **Automated Scanning:** Schedule regular vulnerability scans on all critical systems to detect newly discovered risks.
2. **Risk Dashboard:** Implement a centralized dashboard to log identified risks, their CVSS scores, treatment status, and deadlines.
3. **Change Management Alerts:** Track updates from Microsoft for newly released patches or exploits. Subscribe to security advisories for relevant products.
4. **Review Cycle:** Review mitigated risks quarterly to ensure patch integrity and to validate that no residual vulnerabilities remain.
5. **Audit Logs:** Analyze system logs for signs of intrusion attempts related to identified vulnerabilities.