Leapmile - Vulnerability and Patch Management Process

Effective Date: May 1, 2025

Purpose & Scope: To ensure that all layers of the IT environment—including Operating Systems (OS), Databases (DB), Middleware, and Applications—are regularly assessed and updated to mitigate security vulnerabilities and support an immediate response to critical threats. This process applies to all systems, applications, services, and infrastructure components managed by the organization, whether on-premise or in the cloud.

Definitions

Vulnerability: A weakness in a system or software that can be exploited to compromise the integrity, confidentiality, or availability of information or resources.
Patch: A software update intended to fix security vulnerabilities and/or improve performance.
Critical Vulnerability: Any security flaw that poses a high risk of exploitation with severe potential impact; typically rated as CVSS score ≥ 7.0.

Key Principles

The organization has designed its systems with appropriate built-in safeguards to mitigate common security threats.
Internal assessments are conducted, even though external penetration testing services are not currently engaged. The goal is to have a discovery process in place to identify, evaluate, prioritize, and remediate vulnerabilities.

Vulnerability Management Process

Step 1: Identification

Scan the following elements for vulnerability using scanning tools and manual inspections:

- Operating systems
- Databases
- Middleware
- Web and internal applications

Scans are performed:

- Prior to release of each major version for general vulnerabilities
- Immediately when a high or critical vulnerability is disclosed.

Step 2: Evaluation & Prioritization

The IT Security team assesses each vulnerability based on:

CVSS score
Business impact
Exposure (internal vs external)
Critical vulnerabilities are flagged for immediate response.

Step 3: Remediation
Critical vulnerabilities: Must be patched or mitigated within 72 hours of identification.
High vulnerabilities: Addressed within 14 days.
Medium/Low vulnerabilities: Scheduled for patching during the next regular maintenance window or included at next software upgrade.

Step 4: Patch Deployment
Apply patches in test environments first where feasible.
After validation, deploy patches to production systems during maintenance window.
Maintain rollback procedures for any patch application where viable.

5. Patch Management Reporting
Annual reports are generated showing:
Number of vulnerabilities identified by severity
Patching completion timelines and SLA compliance
Pending/unresolved vulnerabilities with justifications

6. Roles and Responsibilities

Role	Responsibility
IT Security Team	Manage vulnerability scans, assess findings, track remediation.
System Owners	Apply patches and confirm resolution.
Change Advisory Board (if applicable)	Review and approve changes for high-impact systems.

Review & Continuous Improvement
The vulnerability and patch management process is reviewed annually or after any major incident.
Industry threat advisories and zero-day exploits are monitored where relevant to ensure secure adaptation.