

Patch Management Report

Author: M.GOKULAN

Internship Research Report

1. Introduction

Patch management is the process of identifying, acquiring, testing, and installing software updates. These updates fix vulnerabilities, improve performance, and enhance security. This report highlights the importance of patch management and best practices.

2. Importance of Patch Management

2.1 Vulnerability Mitigation

Patches address security flaws that attackers can exploit. Unpatched systems are easy targets for cybercriminals.

2.2 System Stability

Software updates often include bug fixes that improve system reliability.

2.3 Compliance

Many standards (PCI-DSS, HIPAA, ISO 27001) require timely patching.

3. Consequences of Not Patching

3.1 Real-World Example: WannaCry Ransomware (2017)

Over 150 countries were affected due to an unpatched Windows vulnerability (MS17-010).

Damages exceeded **\$4 billion** globally.

3.2 Risks of Unpatched Systems

- Ransomware infections
- Data breaches
- System downtime
- Legal penalties
- Exploitation through known vulnerabilities

4. Best Practices for Patch Management

4.1 Maintain an Inventory

Track all hardware and software assets to understand what needs updating.

4.2 Prioritize Critical Patches

Use risk-based prioritization for vulnerabilities scored high in CVSS.

4.3 Test Before Deployment

Deploy patches in a staging environment to check compatibility.

4.4 Automate Where Possible

Use automated patch management tools (e.g., WSUS, ManageEngine, SCCM).

4.5 Regular Audits

Audit systems to verify patch compliance.

4.6 Establish Clear Policies

Define patch timelines, responsibilities, and escalation procedures.

5. Conclusion

Effective patch management is essential to protecting systems from known vulnerabilities. Organizations that apply patches regularly reduce the risk of cyberattacks, improve system performance, and maintain regulatory compliance.