FinalForms Vulnerability and Zero-Day Attack Mitigation Policy

1. Purpose

This policy outlines the approach for managing and mitigating known vulnerabilities and zero-day attack risks within the FinalForms system until patches are available and successfully applied. The goal is to protect sensitive data and ensure service continuity while maintaining compliance with industry standards and best practices for cybersecurity.

2. Scope

This policy applies to all systems, applications, and services managed by FinalForms that are susceptible to vulnerabilities and zero-day exploits. It covers both internal and external-facing components of the system, including but not limited to data storage, user interfaces, and third-party integrations.

3. Definitions

- **Known Vulnerability**: A publicly identified security flaw for which a patch or mitigation may or may not be available.
- **Zero-Day Attack**: An exploit targeting an undiscovered or unpatched vulnerability, for which no immediate fix is available.
- **Patch**: A security update or software fix designed to resolve a vulnerability.
- **Mitigation**: Temporary protective measures taken to reduce risk exposure before a permanent patch can be applied.

4. Roles and Responsibilities

- **CTO (Chief Technology Officer)**: Oversees the identification, assessment, and remediation of vulnerabilities and zero-day risks.
- **CSO (Chief Security Officer)**: Responsible for evaluating the risk associated with vulnerabilities and guiding mitigation efforts.
- **System Administrators**: Implement recommended mitigations and deploy patches once they are available.
- **Business Continuity Team**: Communicates potential risks and mitigation plans internally and to relevant external parties, including customers, if necessary.

5. Vulnerability and Zero-Day Risk Mitigation Procedure

5.1 Identification

1. **Monitoring**: FinalForms continuously monitors for new vulnerabilities through automated security tools, threat intelligence feeds, and regular security assessments.
2. **Notification**: Once a vulnerability is identified, the security team is immediately notified through automated systems, third-party reports, or vendor advisories.

5.2 Risk Assessment

1. **Severity Classification**: Each vulnerability is classified based on its potential impact, using industry-standard risk metrics (e.g., CVSS—Common Vulnerability Scoring System). The vulnerability is categorized as:
   - **Critical**: Immediate threat to sensitive data and system operations.
   - **High**: Significant risk to operations but not immediately exploitable.
   - **Medium**: Possible exposure with limited attack surface.
   - **Low**: Minor risk or unlikely to be exploited.
2. **Impact Analysis**: The security team assesses the potential impact on FinalForms' systems, including:
   - Data integrity and confidentiality.
   - Service availability and uptime.
   - Compliance with data privacy laws and contractual obligations.

5.3 Mitigation

1. **Immediate Actions for Critical Vulnerabilities and Zero-Day Risks**:
   - **Firewall and Network Configuration**: Implement enhanced firewall rules, block or limit access to vulnerable systems, and apply network segmentation to isolate critical components.
   - **Temporary Workarounds**: Disable vulnerable features or services until a patch is available.
   - **Increased Monitoring**: Enable real-time monitoring and alert systems for any suspicious activity or unauthorized access attempts related to the vulnerability.
   - **Rate Limiting**: Apply rate-limiting and DDoS protection where applicable to prevent exploitation.
2. **High-Risk Vulnerabilities**:
   - **Access Control**: Strengthen user authentication measures, including multi-factor authentication (MFA) for affected services.
   - **Patching in Test Environment**: Test available patches in a non-production environment to verify effectiveness and prevent disruption.
3. **Medium and Low-Risk Vulnerabilities**:
   - **Scheduled Patching**: Include patches for lower-risk vulnerabilities in regular update cycles. Monitor for changes in threat level.

5.4 Patch Management

1. **Patch Deployment**: Patches are deployed as soon as they are available. For critical vulnerabilities, patches are prioritized for deployment outside regular maintenance windows to ensure minimal risk exposure.
2. **Testing and Verification**: All patches are tested in a staging environment to verify their stability and effectiveness before being applied to the production environment.

5.5 Post-Mortem and Documentation

After the mitigation process or patch application:

1. **Incident Review**: Conduct a review to assess the effectiveness of the mitigation steps and identify areas for improvement.

2. **Documentation**: All steps taken, including mitigation measures and patch deployment, must be documented and stored in FinalForms’ internal incident tracking system for future reference and audits.

6. Communication Plan

1. **Internal Communication**: The Business Continuity Team will inform relevant staff of any mitigation actions taken and keep them updated on progress.
2. **Customer Communication**: If a vulnerability poses a significant risk to the integrity of customer data or service availability, the Business Continuity Team will issue an advisory to affected customers, outlining the steps being taken to mitigate the issue.

7. Training and Awareness

1. **Staff Training**: All relevant employees, including system administrators and customer support staff, must undergo regular training on vulnerability management and zero-day risk mitigation.
2. **Simulated Drills**: The security team will periodically conduct drills to simulate responses to vulnerabilities and zero-day attacks to ensure readiness.

8. Policy Review and Updates

This policy will be reviewed annually or after any significant incident to ensure its effectiveness. Updates will be made based on the evolving security landscape and the organization's operational needs.

References

- NIST (National Institute of Standards and Technology) Cybersecurity Framework
- CIS (Center for Internet Security) Controls