Vulnerability Management Policy

Purpose

The purpose of this policy is to establish vulnerability management controls and provide guidelines for their implementation. Vulnerability management encompasses source code, operating systems, runtimes, and devices, and vulnerability scans are performed externally via penetration testing and web application scans.

Scope

This policy applies to all systems classified as Customer Confidential as per the Data Classification Policy.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

<Company Name> detects, classifies, tracks and resolves vulnerabilities across all resources and components that comprise <Company Name>'s product and infrastructure. This includes:

- Vulnerabilities in third-party open-source packages
- Common web vulnerabilities such as XSS and injection
- Operating system vulnerabilities on servers and workstations
- Vulnerabilities across self-hosted applications

For each detected vulnerability, <Company Name> assigns severity as follows:

- Critical: The vulnerability can be exploited to gain root or admin access to data and systems containing Customer Confidential or <Company Name> Restricted data, or cause widespread performance degradation. Target resolution: 6-24 hours.
- High: The vulnerability can be exploited to gain unauthorized access to sensitive data, but the exploit is difficult to execute, and requires an additional successful exploit, compromised system, or malfunctioning control. Target resolution: 1-7 days.

- Medium: The vulnerability can be exploited to cause mild performance degradation or to gain access to sensitive data following multiple malfunctioning controls. Target resolution: 7-30 days.
- Low: The vulnerability poses no immediate threat, is highly theoretical, or is not exploitable in the current context. These vulnerabilities may not require manual patching, and are often resolved by following the standard software upgrade process. Target resolution: 30-90 days.

Vulnerability resolution adheres to the standard change management process described in the Change Management Policy.

Any exceptions to resolution windows must be approved by [POLICY OWNER]

and documented as a risk as outlined in the Risk Management Policy.

Pen testing

Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.

<Company Name> compiles the result of each penetration test into a remediation report.

Patch Management

OS patches and docker image updates are applied at least weekly.

<Company Name>s infrastructure employs a variety of virtual machines and containers. Base images for these are retrieved from trusted sources, such as the AWS AMI repository or the Official Images set on dockerhub. Any patches relevant to base images are added to the appropriate build process and deployed to production.

Vulnerability scanning

Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.

In an attempt to prevent vulnerabilities from reaching production environments, <Company Name>utilizes scanning techniques during its development and build processes. Additionally, <Company Name> uses tools to scan its production environment for vulnerabilities not caught by preventative measures. The resolution of any findings is performed in accordance with <Company Name>'s Change Management Policy.