PathwAI

Vulnerability Management Policy

Version 1 - Approved by Abdullah Adeeb

Vulnerability Management Policy

Vulnerability Management is the recurring process of identifying, classifying, prioritizing, mitigating, and remediating security vulnerabilities. This policy focuses on software and system vulnerabilities and the operational vulnerability management process. The process is designed to promote healthy vulnerability/patch management practices and other preventative best practices.

PathwAI Labs utilizes various vulnerability monitoring and scanning systems to help us discover new threats continuously. This policy outlines how we monitor for new vulnerabilities, and how such vulnerabilities are addressed.

Monitoring for Vulnerabilities

1. PathwAI Labs performs various internal vulnerability scans and package monitoring on a continuous basis.
2. PathwAI Labs also performs external vulnerability scans/penetration tests periodically.

Reporting

The Information Security Officer is responsible for communicating detected vulnerabilities and package updates needed to the appropriate vulnerability management system where it can be tracked to resolution.

Remediating Vulnerabilities

Remediation is the part of the process in which a reported vulnerability is fixed. The engineering staff is responsible for remediating any reported vulnerabilities. The remediation process should be tracked in the vulnerability management system. SLAs are in place to help prioritize vulnerability based on severity.

Remediation SLAs

Vulnerabilities are mapped to severity based on a multitude of factors, such as scope, impact, etc. This severity label is used to come up with remediation SLAs.

Remediation Outcomes

The engineering team addresses the reported vulnerabilities and tracks them to resolution. Resolution statuses can include (but are not limited to) the following:

1. Fixed: This means that the reported vulnerability has been fixed via a patch or system changes.
2. Inaccurate/Incorrect/False-positive: This means that the reported vulnerability has been thoroughly investigated, but found to be invalid.

3. Vulnerable-section-unused: This means that the reported vulnerability affects parts of the codebase/system that are not in use, and consequently the vulnerability is no longer a threat.
4. Acceptable-risk: This means that the reported vulnerability has been analyzed and deemed to not pose any debilitating risk to the system. This is a rare case scenario, and should only occur when there are extenuating circumstances or extremely high remediation costs.

Non-Compliance

As stated earlier, our customers and other stakeholders depend on us to protect their data. In order to uphold their trust in us, it is important to have appropriate penalties for any violations of this policy. PathwAI Labs management will determine how serious an employee's offense is and decide the appropriate penalty. Penalties may include a warning (oral/written) or suspension or termination for more serious offenses.

Questions

If you have any questions regarding this policy, please reach out to the policy owner.

End of Vulnerability Management Policy.For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Abdullah Adeeb	02 Dec, 2025
1		New policy version created	02 Dec, 2025