Coordinated Vulnerability Disclosure Policy

Aklivity, Inc.

Version: 1.0

Effective Date: January 6, 2025

Contact: security@aklivity.io

1. Introduction

Aklivity is committed to ensuring the security of our software and ecosystem. We recognize the important role that independent security researchers and the broader community play in identifying potential vulnerabilities. This Coordinated Vulnerability Disclosure Policy outlines our approach to receiving and responding to security reports in a responsible and timely manner.

2. Scope

This policy applies to:
- Aklivity's open-source and commercial software (e.g., Zilla, Zilla Plus).
- Docker containers and artifacts published by Aklivity.
- Documentation, configuration templates, and sample deployments.
- Publicly accessible domains under aklivity.io.

Out of scope:
- Third-party dependencies not maintained by Aklivity.
- Self-hosted deployments that are fully customer-controlled.

3. Reporting a Vulnerability

To report a security vulnerability, please contact us at:

 security@aklivity.io

Please include:
- A clear and concise description of the issue.
- Steps to reproduce (including proof-of-concept if available).

- Impact assessment and any known mitigations or workarounds.
- Your contact information (PGP key if encrypted communication is preferred).

Optional: Encrypt your report using our PGP key available at https://aklivity.io/security.

4. What to Expect

Once a report is received:
1. Acknowledgment: We'll acknowledge receipt within 3 business days.
2. Triage: We will validate the report and assess its impact.
3. Coordination: If confirmed, we will coordinate a remediation timeline and credit the reporter (with permission).
4. Resolution: Patches or updates will be issued as soon as reasonably possible.
5. Disclosure: We aim to disclose confirmed vulnerabilities within 90 days of initial report, unless otherwise agreed upon.

5. Responsible Research Guidelines

We request that researchers:
- Do not exploit the vulnerability beyond what is necessary to demonstrate the issue.
- Do not access, modify, or delete customer or system data.
- Do not perform denial-of-service attacks or impact availability.
- Give Aklivity adequate time to investigate and remediate before public disclosure.

We will not pursue legal action against individuals who discover and report vulnerabilities in good faith and follow this policy.

6. Recognition

We appreciate the contributions of ethical security researchers. With permission, we may offer:
- Public acknowledgment on our security page.
- Swag or other discretionary rewards for significant or high-impact findings.

7. Policy Changes

This policy may be updated from time to time. The latest version will always be available at:
🔗 https://www.aklivity.io/security