Jiko Securities, Inc.

Jiko Vulnerability Disclosure Policy

June 24, 2024

We take the security of our systems seriously, and we value the security community. The disclosure of security vulnerabilities helps us ensure the security and privacy of our users and systems.

Guidelines

We require that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing;
- Perform research only within the scope set out below;
- Use the identified communication channels to report vulnerability information to us; and
- Keep information about any vulnerabilities you've discovered confidential between yourself and Jiko until we've had 90 days to resolve the issue.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research;
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission);
- Recognize your contribution with a monetary reward, if you are the first to report the issue and we make a code or configuration change based on the issue.

In-Scope Vulnerabilities

The following types of vulnerabilities are considered within the scope of our security vulnerability program:

- **Account Takeover**
    - Vulnerabilities that allow an attacker to gain control of another user's account through methods such as credential theft, session hijacking, or bypassing authentication mechanisms.

- **Unauthorized Access to Data**
    - Issues that allow access to data that does not belong to the account in question, including:
        - Accessing another user's personal information.
        - Viewing or modifying another user's account settings or data.
        - Extracting sensitive data such as payment information, personal identification information (PII), or other confidential information.
- **Injection Vulnerabilities**
    - Vulnerabilities such as SQL injection, command injection, and other forms of code injection that can lead to unauthorized data access or manipulation.
- **Authentication and Authorization Flaws**
    - Weaknesses that allow bypassing authentication or authorization mechanisms, leading to unauthorized access to resources or data.
- **Security Misconfigurations**
    - Incorrectly configured security settings that expose sensitive data or functionalities to unauthorized users.
- **Sensitive Data Exposure**
    - Unintended exposure of sensitive data through API responses, error messages, or other means.
- **Server-Side Request Forgery (SSRF)**
    - Vulnerabilities that allow an attacker to make arbitrary requests from the server, potentially leading to internal network access or data extraction.

Out-of-Scope Vulnerabilities

The following types of vulnerabilities are generally considered out of scope for our security vulnerability program:

- **Denial of Service (DoS)**
    - Issues that cause temporary unavailability of services but do not lead to data breaches or security bypasses.
- **Spamming Techniques**
    - Issues related to email or message spam without an associated security impact.
- **Social Engineering**
    - Attacks that require deceiving individuals rather than exploiting technical vulnerabilities.
- **Physical Attacks**
    - Vulnerabilities requiring physical access to premises or devices.
- **Issues with Third-Party Services**
    - Vulnerabilities in services not directly managed or controlled by Jiko.
- **Non-Exploitable Vulnerabilities**
    - Theoretical vulnerabilities with no practical exploitability or security impact.

- **Full Access Requirements**
    - Vulnerabilities that require full access to a customer's mobile device or email account. Such issues are not considered vulnerabilities within our systems but rather a breach of personal security.

Reporting Guidelines

When reporting vulnerabilities, please provide as much detail as possible, including:

- Steps to reproduce the vulnerability.
- Potential impact and severity of the vulnerability.
- Any relevant screenshots, video recordings, logs, or evidence.

Things we do not want to receive:

- Personally identifiable information (PII)
- Credit card holder data

How to report a security vulnerability?

If you believe you've found a security vulnerability or a compliance issue in one of our products or platforms please send it to us by emailing **security@jiko.io**.