zepto

1300 611 406 zepto.com.au 11 March 2025

VULNERABILITY DISCLOSURE POLICY

Zepto's preferences for disclosure when Researchers discover vulnerabilities within our platform, and guidance to what we consider good faith security Research.

Introduction

Zepto Payments Pty Ltd ("**Zepto**", "**we**", "**us**" or "**our**") is committed to ensuring the security of both our users and customers by protecting their information and services. This policy is intended to:

a) Convey our preferences for disclosure when Researchers discover vulnerabilities within our platform; and
b) Provide guidance with regards to what we consider good faith security Research,

(the "**Policy**").

If you adhere to the directives in this Policy, act in good faith and abide by applicable laws, Zepto will be more inclined to authorize your Research in accordance with ISO/IEC 29147:2018.

This Policy describes:

a) The **systems and types of Research** that are covered under this policy;
b) **How to send us** vulnerability reports;
c) **How long** we ask security researchers to wait for publicly disclosing vulnerabilities; and
d) **How we acknowledge** and award discoveries.

In this Policy, the following definitions apply:

"**Research**" is defined as activities you undertake to discover, analyse, confirm and report vulnerabilities relating to our platform.

"**Researcher**" means a person or entity undertaking Research.

Authorisation

If you make a good faith effort to comply with this policy during your security Research, we will consider authorizing your Research, we will do our best to work with you to understand and resolve the issue quickly, and Zepto may not recommend or pursue legal action related to your research.

Should legal action be initiated by a third party against you for activities that were conducted in accordance with this Policy, subject to any applicable laws, we will make this authorisation known.

Guidelines

In the context of this Policy, when undertaking Research activities, you must:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every reasonable effort to avoid violating any privacy laws, affecting our customers' and users' experience, disruption of production and critical systems and the destruction, corruption or manipulation of data.
- Limit the use of exploits to the extent necessary to confirm a vulnerability's presence. Do not use such exploits to:
    - a) Compromise systems
    - b) Exfiltrate data
    - c) Establish persistent access
    - d) Pivot to other systems or infrastructure
- Provide us a reasonable amount of time to resolve the issue before public disclosure by yourself
- Not submit a high volume of low-quality or insufficiently detailed reports.

The moment you have established that a vulnerability or issue exists or encounter any sensitive data (including any personal information, financial information, proprietary information or trade secrets of any party), **you must immediately stop your test, notify us without delay and must not disclose this data to anyone.**

Test methodologies

The following methods are not covered within this policy and will not be subject to any protections afforded here:

- **Denial of Service** via network (e.g. DoS or DDos) or other tests that impair access to our systems via volumetric, technical or other means.
- **Social Engineering**, this includes but isn't limited to phishing emails and other digital phishing attempts.
- **Physical testing** (e.g. accessing our offices, open doors, tailgating) or any other non-technical vulnerability testing.

Scope

This policy applies to the following systems and services:

- sandbox.zeptopayments.com
- *.sandbox.zeptopayments.com
- 13.237.142.60

We do understand that in the normal course of use or evaluation of our products that there is a potential for identification of reportable issues. As such, when vulnerabilities are identified in production systems **you must immediately cease testing** and if possible, **collect relevant reporting evidence on sandbox systems.**

For posterity and to aid with avoiding testing against them, our production systems are found at:

- api.zeptopayments.com
- go.zeptopayments.com
- 52.64.11.67

- 13.238.78.114

Vulnerability severity ratings

To simplify reporting vulnerabilities, we have adapted a vulnerability reporting taxonomy similar to those used in traditional bounty programs.

This classifies vulnerabilities using a severity of 1-5 where:

- 1 is the highest severity; and
- 5 is the lowest severity.

Please note: that the priority and severity of a reported vulnerability **is not confirmed nor accepted until Zepto validates the severity rating.**

Reporting a vulnerability

We currently accept vulnerability reports via the email address: researchers@zepto.com.au (**please check https://zepto.com.au/security.txt to ensure you have up to date information**). Reports may be submitted anonymously to the extent email allows, however, Zepto will not provide acknowledgement or rewards (if any) where contact information is not provided. **We will acknowledge receipt by email within 3 business days.**

We support and encourage the use of Pretty Good Privacy ("**PGP")** encryption for vulnerability reports, for which relevant keys and within our security.txt file at: https://zepto.com.au/security.txt

What we would like to see from you

To ensure we can triage and prioritise your submission with the level of urgency relevant to the vulnerability, reports must include the following information:

- Where the vulnerability was discovered
    - In the case of web applications, this should include relevant URL paths and query strings
- An overview of the impact and threat posed by the vulnerability
    - This can include, for example, attack trees or paths highlighting how attackers may exploit the vulnerability
- A detailed description of the steps needed to reproduce the vulnerability, including but not limited to:
    - Proof of concept exploits
    - Screenshots
    - Tool data outputs

Our security team converses and works in English. Vulnerability reports must therefore be provided in English, so as to ensure we are responding in the correct manner.

What you can expect from us

You can expect us to:

- Acknowledge receipt within 3 business days;
- If we agree with your Research, and to the best of our ability, we will confirm the existence of the vulnerability to you and outline the steps of our proposed remediation process, including situations where there are issues and challenges;
- Use our best efforts to maintain an open and active dialogue with you;
- Provide a token of our gratitude in the form of a reward (which may not be monetary); and

In certain circumstances, we may also publicly acknowledge your discovery (if you so desire).

Questions

If you have any questions or concerns about this policy please contact us via researchers@zepto.com.au. We also invite suggestions for improving this policy.