Vulnerability Disclosure Program

Introduction

Vulnerability Disclosure Program for Wizzit. Our security team is committed to protecting our user community and ensuring the integrity of our systems. We recognize the value that the research community offers and invite you to participate in our program. This page outlines our guidelines for disclosing vulnerabilities responsibly.

Program Scope

What is in Scope

- Latest public versions of all Wizzit payment services

What is Out of Scope

- Non-Security related bugs
- Social engineering
- Phishing
- Email Spoofing
- Previously Reported Security related vulnerabilities
- Test or beta applications
- Third party applications or libraries not owned by Wizzit.
- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks
- Physical attacks against company property or data centres

Submission Guidelines

How to Submit a Vulnerability

Please report vulnerabilities by sending a detailed email to wizzit_vdp@wizzit.com. Your report should include:

- **Summary**: A description that provides a quick understanding.
- **Reproduction Steps**: A guide on how the vulnerability can be reproduced. This will aid the IT team in verifying and addressing the vulnerability.
- **Impact**: A section to describe potential consequences.
- **Proof of Concept (PoC):** Any evidence like scripts or screenshots.

- **Supporting Materials**: Additional references or materials.
- **Environment Details**: Information about where the vulnerability was discovered, such as Endpoints, client, App version, SDK version etc.
- **Researcher Contact**: Details of the individual or team who identified the vulnerability.

What to Expect After Submission

- **Acknowledgment**: We will confirm the receipt of your report within 48 hours.
- **Unique Case ID**: A tracking number will be assigned to your submission for future correspondence.

Safe Harbor

Safe Harbor provisions are designed to protect well-intentioned security researchers from legal actions as a result of their discoveries. The following outlines our Wizzits's position on this and provides guidelines for how we'll handle these scenarios.

Good Faith Requirement

- A researcher is considered acting in "good faith" if they:
    - Adhere strictly to our Vulnerability Disclosure Policy.
    - Avoid accessing, downloading, or modifying data that doesn't belong to them.
    - Refrain from disclosing vulnerability details to the public before we address them.

Do not use the vulnerability to cause harm or to exploit it beyond what's strictly necessary to demonstrate it.

Our Commitment

If a researcher meets the "good faith" criteria:

- We commit to not initiating any legal action related to their research.
- We will not recommend or support any third-party legal actions against the researcher.
- We'll work to address the reported vulnerabilities in a timely and responsible manner.

Exceptions to Safe Harbor

While we strive to be fair, certain activities will void the Safe Harbor protection:

- If a researcher performs Denial of Service (DoS) attacks.

- If they access, modify, or delete user data (unless explicitly permitted by the user).
- If they violate any other explicit restrictions outlined in our policies.

Response Times and Resolution

- **Initial Review**: Within 10 business days after acknowledgment.
- **Updates**: Weekly updates until the issue is resolved.
- **Resolution**: Timeline may vary depending on the severity and complexity of the identified issue.

No Monetary Rewards

Although we do not currently offer financial rewards, we are deeply appreciative of your efforts and will acknowledge your contributions in internal bulletins and, if you consent, in public communications.

Selective Disclosure Policy

We will first notify directly affected customers and stakeholders prior to broader disclosure. Researchers are expected to honor this disclosure strategy.

Feedback on the Program

Feedback helps us improve. If you have suggestions on how we could improve this program, please email wizzit_vdp@wizzit.com.

Contact Information

- Vulnerability Reports: wizzit_vdp@wizzit.com
- Feedback: wizzit_vdp@wizzit.com
- Legal Concerns: legal@wizzit.com

Thank you for helping us maintain the security and integrity of our systems. We look forward to your participation.