Dash0 Vulnerability Disclosure Policy

Last updated February 13, 2024

Table of Contents

Introduction

At Dash0, we take the security of our systems and products seriously. We recognize the valuable role that security researchers and the wider security community play in helping us identify and address potential vulnerabilities. This Vulnerability Disclosure Policy outlines the guidelines and procedures for reporting security issues or vulnerabilities in our systems, products, or services.

Scope

This policy applies to all Dash0 services, products, websites, and systems. If you discover a potential security vulnerability, we encourage you to report it in accordance with the guidelines provided here.

Reporting Security Vulnerabilities

If you believe you have identified a security vulnerability in any of our services or products, we encourage you to report it to us promptly. To report a vulnerability, please follow these steps:

- Contact Information: Send an email to security@dash0.com. Please use the subject line "Security Vulnerability Report" to ensure a swift response.

- Provide Details: In your report, please include a detailed description of the vulnerability, including its potential impact and any technical information or proof of concept that demonstrates the vulnerability.
- Your Contact Information: Please provide your contact information, including your name, email address, and any other preferred means of contact. This allows us to communicate with you and provide updates regarding the resolution of the reported issue.
- Responsible Disclosure: We kindly request that you follow responsible disclosure practices by not sharing or disclosing the vulnerability with third parties until we have had a reasonable opportunity to address it.

Expectations from Dash0

Upon receiving your report, we commit to the following:

- Acknowledgement: We will acknowledge receipt of your report as soon as possible.
- Investigation: Our security team will investigate and verify the reported vulnerability's validity. If necessary, we may request additional information or clarification from you.
- Resolution: We will work diligently to address and resolve the reported vulnerability in a timely manner.
- Communication: We will maintain open and transparent communication with you throughout the process and notify you of the resolution status.
- Credit and Recognition: If you wish to be credited for your responsible disclosure, we will acknowledge your efforts publicly upon request.

Our Commitment

We are committed to protecting our users' data and ensuring the security of our systems and products. We take all reports of security vulnerabilities seriously and will address them promptly. We appreciate the contributions of security researchers and the security community in helping us maintain the highest security standards.

Responsible Disclosure

We encourage security researchers and reporters to adhere to responsible disclosure practices. This helps us protect our users and ensure the effectiveness of our security measures. We ask that you:

- Avoid any malicious activities or exploitation of the reported vulnerability.
- Keep all communication confidential until a resolution has been reached.
- Do not disclose the vulnerability to any third party without our consent.

Legal Protections

We will not initiate any legal action against security researchers or reporters for good-faith vulnerability disclosure. Your actions in reporting security vulnerabilities are protected under the law.

Feedback and Questions

If you have any feedback or questions regarding our Vulnerability Disclosure Policy, please feel free to contact us at security@dash0.com.

Policy Updates

This policy may be updated from time to time to reflect changes in our security practices or the technology landscape. Please review this policy periodically for any updates.

Effective Date

This Vulnerability Disclosure Policy is effective as of the date of last update mentioned at the beginning of this document.

Thank you for your assistance in helping us maintain the security and integrity of our services and products. We appreciate your collaboration in making the internet a safer place.