LOVESTOCK
& LEAF

Responsible Disclosure Policy

Last Updated: 13 August 2020

App Security Responsible Disclosure Policy for Lovestock & Leaf

Introduction

Lovestock & Leaf aims to keep its apps safe for everyone, and data security is of utmost priority. If you are a security researcher and have discovered a security vulnerability in the apps, we appreciate your help in disclosing it to us in a responsible manner.

We appreciate the assistance and patience of security researchers and are committed to reviewing all reports that are disclosed to us. We will do our best to address each issue in a timely fashion, and request that you provide us with a reasonable timeframe to address the issue before public disclosure.

Please do not publicly disclose the details of any potential security vulnerabilities without express written consent from us.

To encourage responsible disclosure, we will not take legal action against security researchers in relation to the discovery and reporting of a potential security vulnerability. This is provided that all such potential security vulnerabilities are discovered and reported strictly in accordance with this Responsible Disclosure Policy. In the event of any non-compliance, we reserve all of our legal rights.

How to report a potential security vulnerability

You can responsibly disclose potential security vulnerabilities to the Lovestock & Leaf Security Team by emailing security@lovestockleaf.com. Ensure that you include details of the potential security vulnerability and exploit with enough information to enable the Security Team to reproduce your steps.

What to include in your report

When reporting a potential security vulnerability, please include as much information as possible, including:

- Vulnerable URL - the endpoint where the vulnerability occurs;
- Vulnerable Parameter - if applicable, the parameter where the vulnerability occurs;
- Vulnerability Type - the type of the vulnerability;
- Steps to Reproduce - step-by-step information on how to reproduce the issue
- Screenshots or Video - a demonstration of the attack; and
- Attack Scenario - an example attack scenario may help demonstrate the risk and get your issue resolved faster.
- Your contact details
- The names of any test accounts you have created (where applicable)

Testing Exclusion

In no event are you permitted to access, download or modify data residing in any other Account, or one that is not registered to you. We will not honor any issues which result from testing our customers. All research must be conducted using your own Zendesk instance where you can sign up for here; and sign up to your own subscription to our apps via the Zendesk marketplace here.

You are also prohibited from:

- Attempting to social engineer Lovestock & Leaf staff.
- Executing or attempting to execute any Denial of Service attack.
- Knowingly posting, transmitting, uploading, linking to, sending or storing any Malicious Software.

- Testing in a manner that would result in the sending of unsolicited or unauthorized junk mail, spam, pyramid schemes or other forms of duplicative or unsolicited messages.

Authorised	
Name: Mark Heath, Director	
Signature:	
Date: 13 August 2020	
Date of next review: 13 August 2021	