Responsible Disclosure Policy

Read Naturally, Inc.

Purpose

To allow for the reporting and disclosure of vulnerabilities discovered by external entities, and anonymous reporting of information security policy violations by internal entities.

Scope

Read Naturally, Inc.'s Responsible Disclosure Policy applies to Read Naturally, Inc.'s core platform and its information security infrastructure, and to internal and external employees or third parties.

Background

Read Naturally, Inc. is committed to ensuring the safety and security of our customers and employees. We aim to foster an environment of trust, and an open partnership with the security community, and we recognize the importance of vulnerability disclosures and whistleblowers in continuing to ensure safety and security for all of our customers, employees and company. We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

Roles and Responsibilities

Read Naturally, Inc.'s CTO is responsible for enforcing this policy.

Legal Posture

Read Naturally, Inc. will not engage in legal action against individuals who submit vulnerability reports through security@readnaturally.com. We openly accept reports for the currently listed Read Naturally, Inc. products. We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming Read Naturally, Inc. or its customers.
- Engage in vulnerability testing within the scope of our vulnerability disclosure program.
- Test on products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhere to the laws of their location and the location of Read Naturally, Inc. For example, violating laws that would only result in a claim by Read Naturally, Inc. (and not a criminal claim) may be acceptable as Read Naturally, Inc. is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public before a mutually agreed-upon timeframe expires.

Policy

Vulnerability Report/Disclosure

How to Submit a Vulnerability

To submit a vulnerability report to Read Naturally, Inc.'s Security Team, please utilize the following email: security@readnaturally.com.

Preference, Prioritization, and Acceptance Criteria

We will use the criteria from the next sections to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English will have a higher probability of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from Read Naturally, Inc.:

- A timely response to your email (within 2 business days).
- After triage, we will send an expected timeline and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.

If we are unable to resolve communication issues or other problems, Read Naturally, Inc. may bring in a neutral third party to assist in determining how best to handle the vulnerability.

- Corrective actions taken to resolve a verified violation and a review and enhancement of applicable policies and procedures, if necessary or appropriate.
- Continuous information security awareness training and understanding your rights as a whistleblower.

Revision History

Version	Date	Editor	Approver	Description of Changes
1.0	12-9-2024	Security Team	Puneet Sinha	Initial creation of policy