Security and Compliance

Overview

This document provides an overview of the responsible disclosure program at Boxabl, also known as a ‘bug bounty’ program. Boxabl supports and rewards security researchers acting in good faith to help us improve the security of our products and services through responsible disclosure, provided those disclosures are made in accordance with the terms and conditions in this policy.

Before submitting any finding to this program, you must read and understand the contents of this policy fully.

In return, Boxabl offers compensation based on our internal assessment of the severity of any discovered issue. **All rewards are entirely at our discretion.**

Scope

The following Boxabl software products are in scope:

- The Boxabl marketing site: www.boxabl.com
- Any publicly exposed infrastructure elements that support Boxabl’s product or business operations.

Absolutely not in scope:

- Third party business applications leveraged by Boxabl.
- Non-production environments, unless their vulnerabilities directly impact production environments.

The following vulnerability types are not considered in-scope unless our implementation has resulted in data leakage or account takeover:

- Configuration and best practices such as SPF/DMARC, CORS, security headers, or insecure SSL/TLS ciphers.
- Denial of Service.
- Information disclosure such as file path, unless it can lead to sensitive info.
- Clickjacking.
- Email and account policies such as reset method and password complexity.
- Theoretical XSS or self-XSS attacks without evidence of exploitability, such as input being reflected in response.

Rules of Engagement and Legal Matters

Boxabl will not engage in legal action against individuals or entities that submit vulnerability reports that cover in scope products and services (as defined above), through the approved channels (defined below).

Furthermore, Boxabl agrees not to pursue legal action against individuals or entities that adhere to the following rules of engagement when identifying and submitting vulnerabilities:

- Testing and/or research should be non-disruptive (e.g. no denial of service), and should not harm Boxabl's operations or customers. If you're not sure if a particular test will cause disruption, err on the side of caution and do not perform it without consulting Boxabl's security team first.
- Testing and/or research should be on in scope systems only. If you're not sure whether a system is in scope, please ask.
- Testing and/or research should not deliberately seek to access information belonging to Boxabl customers. Instead, a researcher should leverage their own accounts within the Boxabl environment.
- Security researchers should refrain from disclosing issues publicly prior to a mutually agreed upon disclosure date.
- Security researchers are responsible for ensuring they always adhere to local laws and legislation.
- All security researchers wishing to be considered for compensation when submitting a vulnerability should ensure that their research, or testing, is conducted in accordance with the above rules of engagement.

How to Report a Vulnerability to Boxabl

Vulnerability reports should be submitted to the Boxabl security team via email to bugs@boxabl.com.

Preference, Prioritization and Acceptance Criteria

In order to obtain the most value from this program, for both Boxabl and the participating security researcher, we strongly advise that, and will give priority to disclosures which include:

- Reports that are well written, and submitted in English where possible.
- Reports that include proof of concept code that permit Boxabl to better triage the issue.
- Reports that include details of how the vulnerability was identified, a suggested impact rating, and any potential remediations you might suggest.
- Reports that are more than just output from automated testing tools, and scans.
- Reports that include any intentions or timelines for public disclosure.

If you follow these guidelines, you can expect the following from Boxabl:

- A timely response to your initial disclosure.
- Open dialog which includes planned remediation timelines where a remediation is necessary.
- Notification when final remediation has occurred.
- Compensation where applicable (see below).

Compensation

Boxabl compensates security researchers based on the following factors:

The severity of the issue identified (we leverage a formula linked to the CVSS).

- The quality of the reporting.
- Boxabl's internal risk assessment of the issue.
- Whether or not the issue has already been disclosed to Boxabl prior to your submission (we only pay out once per issue).
- Any applicable legislation that may impact our ability to award compensation, for example, international sanctions against individuals or countries.

Boxabl will work with the researcher to facilitate payment. Payment amounts are entirely at Boxabl's discretion — which is something you agree to when submitting bugs as part of this program.