Appcues, Inc Vulnerability Disclosure Policy

January 2023

Introduction

Appcues, Inc welcomes feedback from security researchers and the general public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you. This policy outlines steps for reporting vulnerabilities to us, what we expect, and what you can expect from us.

Systems in Scope

This policy applies to any digital assets owned, operated, or maintained by Appcues, Inc.

Out of Scope

Assets or other equipment not owned by parties participating in this policy. Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or applicable authority.

Our Commitments

When working with us, according to this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed;
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints; and
- Extend Safe Harbor for your vulnerability research that is related to this policy.

Our Expectations

In participating in our vulnerability disclosure program in good faith, we ask that you:

- Play by the rules, including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail;
- Report any vulnerability you've discovered promptly;
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience;
- Use only the Official Channels to discuss vulnerability information with us;
- Provide us a reasonable amount of time (at least 90 days from the initial report) to resolve the issue before you disclose it publicly;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information;
- You should only interact with test accounts you own or with explicit permission from the account holder; and
- Understand when submitting reports there is no monetary compensation at this time;
- Do not engage in extortion.

Official Channels

Please report security issues via mailto:security@appcues.com, providing all relevant information. The more details you provide, the easier it will be for us to triage and fix the issue.