Vulnerability Disclosure Program

APP IN THE AIR INC.

Overview

App in the Air is committed to protect the privacy and security of users of our service. The Vulnerability Disclosure Program is intended to minimize the impact any security flaws have on the products and users of the company.

Purpose

The purpose of this program is to fix security vulnerabilities. Other bugs will be accepted at our discretion and can be reported via any appropriate channel: via the app's internal tools or emailing to support@appintheair.mobi.

Scope

All the products of App in the Air are in scope. The products include but not limited to Websites, iOS apps, Android apps. The vulnerability must exist in the latest public release (including officially released public betas) of the product.

Guidelines

App in the Air agrees to not pursue civil claims against researchers related to the disclosures submitted according to the following guidelines:

- Researches should not permanently modify or delete App in the Air-hosted data.
- Researches should not intentionally access non-public App in the Air data any more than is necessary to demonstrate the vulnerability.
- Researches should not DDoS or otherwise disrupt, interrupt or degrade App in the Air internal or external services.
- Researches should not share confidential information obtained from App in the Air, including but not limited to users' data, trips information, and credentials.
- Researchers should provide a detailed summary of the vulnerability, including the target, steps, tools, and artifacts used during discovery necessary to reproduce the vulnerability.
- Researchers should comply with all applicable laws.

In addition, App in the Air will put the best efforts to fix the vulnerability within 30 days before publicly announcing it. App in the Air believes that security researchers have a First Amendment right to report their research and that disclosure is highly beneficial, and understands that it is a highly subjective question of when and how to hold back details to mitigate the risk that vulnerability information will be misused.

Out of scope

- Reports from automated tools or scans
- Issues without clearly identified security impact (such as clickjacking on a static website), missing security headers, or descriptive error messages
- Missing best practices, information disclosures, use of a known-vulnerable libraries or descriptive / verbose / unique error pages (without substantive information indicating exploitability)
- Speculative reports about theoretical damage without concrete evidence or some substantive information indicating exploitability
- Self-exploitation
- Missing security-related HTTP headers which do not lead directly to a vulnerability
- Self cross-site Scripting vulnerabilities without evidence on how the vulnerability can be used to attack another user
- Social engineering of App in the Air employees or contractors
- Denial of Service Attacks
- HTML content injection
- Attacks requiring MITM or physical access to a user's device

Reporting

Just as important as discovering security flaws is reporting the findings so that users can protect themselves and vendors can repair their products. Public disclosure of security information enables informed consumer choice and inspires vendors to be truthful about flaws, repair vulnerabilities, and build more secure products.

On the other hand, vulnerability information can give attackers who were not otherwise sophisticated enough to find the problem on their own the very information they need to exploit a security issue and cause harm. Therefore, App in the Air asks researchers to privately report the vulnerability before public disclosure.

Vulnerabilities can be reported to vulnerability@appintheair.mobi with information about the vulnerability and detailed steps on how to replicate it according to the Guidelines indicated within the Program.