Vulnerability Disclosure Policy

Airbase is committed to providing a robust and secure service to our customers and maintaining the security, confidentiality, availability, privacy, and integrity of our products is a priority at Airbase. Therefore, Airbase appreciates the work of researchers in order to improve our security and/or privacy posture. We are committed to creating a safe, transparent environment to report vulnerabilities.

If you have come across a security or privacy vulnerability that could impact Airbase or our customers, we encourage you to report this immediately at security@airbase.io. We will investigate all valid reports and fix the vulnerability as soon as we can. We encourage you to follow Airbase's Vulnerability Disclosure Policy and make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service during your research.

Scope

Services that Airbase provides or any Airbase product are in scope. The following are excluded from the Responsible Disclosure Policy (note that this list is not exhaustive):

- Taking any action that may negatively affect Airbase.
- Retaining any personally identifiable information discovered, in any medium. Any personally identifiable information discovered must be permanently destroyed or deleted from your device and storage.
- Disclosing any personally identifiable information discovered to any third-party application/systems.
- Destruction or corruption of data, information or infrastructure, including any attempt to do so.
- Reconnaissance dependent on social engineering techniques of any kind (any verbal or written interaction with anyone affiliated with or working for Airbase).
- Any exploitation actions, including accessing or attempting to access Airbase's data or information, beyond what is required for the initial "Proof of Vulnerability." The actions to validate the Proof of Vulnerability must stop immediately after initial access to the data or a system.
- Attacks on third-party services.
- Denial of Service (DoS) attacks or Distributed Denial of Services (DDoS) attacks.
- Use of assets that you do not own or are not authorized or licensed to use when discovering a vulnerability.
- Knowingly posting, transmitting, uploading, linking to, or sending any viruses/malware.
- Pursuing vulnerabilities that send unsolicited bulk messages (spam) or unauthorized messages.
- Any vulnerability obtained through the compromise of Airbase customer or employee accounts.
- UI and UX bugs and spelling mistakes.

Out of scope vulnerabilities

- Vulnerabilities identified with automated tools (including web scanners) that do not include proof-of-concept or a demonstrated exploit.
- Third-party applications or services that integrate with Airbase.
- Discovery of any third-party services (vulnerable third-party code) whose running version includes known vulnerabilities without demonstrating an existing security impact.

Eligibility and disclosure

Eligibility:

- You must agree to our Vulnerability Disclosure Policy.
- You must be the first person to responsibly disclose an unknown issue.

Airbase pledges not to initiate any legal action against researchers if they adhere to the guidelines outlined in our Vulnerability Disclosure Policy. In order to protect our customers, Airbase requests that you not post or share any information about a potential vulnerability in any public forums/sites until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed.

As mentioned in our Privacy Policy, Airbase's website and services are not intended for, or designed to attract, individuals under the age of 18. Due to the Children's Online Privacy Protection Act (COPPA), we cannot accept submissions from children under the age of 13.

This program is not open to any individual on, or residing in any country on, any U.S. sanctions lists.

The decision to pay a reward is entirely at our discretion. You must not violate any law. You are responsible for any tax implications or additional restrictions depending on your country and local law. We reserve the right to cancel this program at any time.

Acceptance criteria

We will use the following criteria to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English with steps on how to reproduce.
- Reports that include proof-of-concept code along with the use of the exploit.
- Reports that only include automated tool output may receive lower priority.
- Reports should include how you found the bug, the impact, and potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from us:

- A timely acknowledgment of your email.
- We will share the expected timeline to fix the vulnerability, after triage. We will be as transparent as possible about the remediation status and reasons that may extend it.
- An open dialogue to discuss issues.
- Notification when the vulnerability has been remediated.
