Responsible Disclosure Program

Allbirds is committed to maintaining the security of our systems and our customers' information. We appreciate and encourage security researchers to contact us to report potential vulnerabilities identified in any product, system, or asset belonging to Allbirds.

If you believe you have identified a potential security vulnerability, please share it with us by following the submission guidelines below. Thank you in advance for your submission, we appreciate researchers assisting us in our security efforts.

Please note, Allbirds does not operate a public bug bounty program and we make no offer of reward or compensation in exchange for submitting potential issues.

Responsible disclosure program guidelines

Researchers shall disclose potential vulnerabilities in accordance with the following guidelines:

1. Do not engage in any activity that can potentially or actually cause harm to Allbirds, our customers, or our employees.
2. Do not engage in any activity that can potentially or actually stop or degrade Allbirds services or assets.
3. Do not engage in any activity that violates (a) federal or state laws or regulations or (b) the laws or regulations of any country where (i) data, assets or systems reside, (ii) data traffic is routed or (iii) the researcher is conducting research activity.
4. Do not store, share, compromise or destroy Allbirds or customer data. If Personally Identifiable Information (PII) is encountered, you should immediately:
    a. Not save, store, transfer, or otherwise access any Allbirds information after initial discovery.
    b. Only view information to the extent required to identify the vulnerability and do not retain information or data.

    c. Only use information obtained from our systems or services to facilitate reporting security vulnerabilities directly to us.
    d. Promptly return any sensitive information or PII and do not retain information or data.
    e. Immediately contact Allbirds
5. Do not initiate a fraudulent financial transaction.
6. Provide Allbirds a reasonable time to fix any reported issue, before such information is shared with a third party or disclosed publicly.

By responsibly submitting your findings to Allbirds in accordance with these guidelines Allbirds agrees not to pursue legal action against you. Allbirds reserves all legal rights in the event of noncompliance with these guidelines.

Once a report is submitted, Allbirds commits to provide prompt acknowledgement of receipt of all reports and will keep you reasonably informed of the status of any validated vulnerability that you report through this program.

Out of scope vulnerabilities

Certain vulnerabilities are considered out of scope for our Responsible Disclosure Program. Out-of-scope vulnerabilities include:

- Physical Testing
- Social Engineering
- Phishing
- Denial of service attacks
- Resource Exhaustion Attacks
- Any other nontechnical vulnerability testing

Submission format

When reporting a potential vulnerability, please include a detailed summary of the vulnerability, including the target, steps, tools, and artifacts used during discovery (screen captures welcome).

Submission instructions

If you wish to report any suspected vulnerability, please privately share full details of the suspected vulnerability by sending an email to infosec@allbirds.com. By including all relevant information in your report, you will enable the Allbirds security team to validate and reproduce the issue and resolve it in a timely manner.