Jasper AI, Inc Vulnerability Disclosure Policy

Introduction

Jasper AI, 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, what you can expect from us.

Scope

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

Jasper being used in ways that violate our terms of use and cause harm….

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, we aim to complete this process within 30 days.
- 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.
- 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 disclosure@jasper.ai email to discuss vulnerability information with us.

- Keep the details of any discovered vulnerabilities confidential until they are authorized for release by the Jasper AI security team. Jasper AI aims to provide the authorization within 90 days of receipt of each report.
- Provide us a reasonable amount of time to resolve the issue.
- 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.
- Only interact with accounts you own.
- Do not engage in extortion.
- Note that Jasper AI does not offer compensation for vulnerability information.
- At Jasper AI, we welcome vulnerability disclosure without conditions attached. While we do not offer monetary compensation for vulnerability information, we appreciate your efforts to help us maintain the highest standards of security. We strictly prohibit any form of extortion, threats, or coercion. Please note that Jasper AI will not provide safe harbor for vulnerabilities shared under threat of public disclosure, data exposure, or non-disclosure.

Out of Scope

The following are non-exhaustively 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).
- Any attacks intended to degrade, deny, or negatively impact services or user experience—such as brute force, denial of service, spamming, and fuzzing—are strictly prohibited, unless given specific permission by Jasper AI.
- Attacks intended to destroy, corrupt, or render data unreadable are strictly prohibited if the data does not belong to you.
- Attacks that exploit stolen or reused credentials, account takeovers, hijacking, and other forms of credential-based activities.
- Deliberately accessing data or information that is not rightfully yours, beyond the bare minimum access necessary to demonstrate a vulnerability.
- The act of physically or electronically gaining access to Jasper AI personnel, offices, wireless networks, or property by means of social engineering, phishing, or any other means is strictly prohibited.
- Attacks linked to email servers, including those associated with email protocols, security measures like SPF, DMARC and DKIM, as well as email-based spam.
- Reports of insecure SSL/TLS ciphers, unless accompanied by a working proof-of-concept.

- Reports of missing HTTP headers (e.g., lack of HSTS), unless accompanied by a working proof-of-concept.
- Reports of iframing on pages with no sensitive/user action is needed.

Official Channels

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

Safe Harbor

When conducting vulnerability research, according to this policy, we consider this research conducted under this policy to be:

- Authorized concerning any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good-faith violations of this policy.
- Authorized concerning any relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls.
- Exempt from restrictions in our Terms of Service (TOS) and/or Acceptable Usage Policy (AUP) that would interfere with conducting security research, and we waive those restrictions on a limited basis.
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws. If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels before going any further.

> Note that the Safe Harbor applies only to legal claims under the control of the organization participating in this policy, and that the policy does not bind independent third parties.

Reporting

Follow this process to report a security issue or vulnerability:

1. Aggregate as much technical information as possible, including steps to reproduce and validate the issue.
2. Within 24 hours of discovery, email your report to the Jasper security team via disclosure@jasper.ai.
3. Allow up to 5 business days for confirmation of the reported issue.