Novelist

1. Introduction

Novelist, a tradename of Amdax B.V., welcomes feedback from security researchers and the 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 would like to hear from you. This policy outlines steps for reporting vulnerabilities to us, what we expect in reporting to us and what you can expect from us in return.

2. Scope

This policy applies to any digital assets owned, operated, or maintained by Amdax B.V. Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be in scope for the program. While this vulnerability disclosure policy primarily represents our focus for security research, we are interested in reports for all our products and services under direct control of Amdax B.V. This can include any open-source libraries, software, or third-party components.

The following subjects are however not in scope, and will not result in a vulnerability disclosure:

- HTTP security headers, including but not limited to CSP, HSTS and X-XSS-Protection;
- Non-200 HTTP return codes;
- Version banners or other service fingerprinting;
- Clickjacking and/or tabnapping;
- Missing Secure/HTTPOnly flags on non-sensitive Cookies;
- E-mail domain and server settings, including DMARC, DKIM and SPF issues;
- Any SSL/TLS issue, including potential weak algorithm support, without a working PoC.

Please note that this policy is **not** an invitation to actively scan our networks or systems for weaknesses in an automated way, causing high loads or traffic on our systems.

3. Our expectations

We expect all security researchers and the public to:

- Act in good faith to avoid privacy violations, degradation of our services, disruption to production systems and destruction of data during security testing;
- Report any vulnerability that is discovered promptly;
- Use only the Official Channels to discuss vulnerability information with us; please report security issues via mail to rd@amdax.com, providing all relevant information. The more details that are provided, the easier it will be for us to triage and fix the issue. Sensitive information should be shared using the following GPG key;
- Perform research only within the scope set out above;
- Only interact with your own accounts or test accounts for security research purposes. Do not access or modify our data or our users' data;
- Keep information about any vulnerabilities that are discovered confidential between us until we have had 90 days to resolve the issue;

- 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, cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII) or other proprietary information.

4. Our Commitments

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

- Respond to your report promptly within 3 business days 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;
- Recognize your contribution to improving our security if you are the first to report a unique vulnerability, and your report triggers a code or configuration change;
- To the extend reasonable or to the extend legally obliged, not to pursue or support any legal action related to your research and findings;
- As a token of appreciation for your help, we will offer a reward for every report of a security problem unknown to us. We will determine the size of the reward based on the severity of the exposed vulnerability and the quality of the report.