Microshare - Security Vulnerability Disclosure Policy

Our Values

Microshare appreciates the valuable work of independent security researchers. We take a serious stance on security and trust, which has led us to develop guidelines on vulnerability reporting. Responsible reporting of vulnerabilities that may be discovered on our site or applications is highly encouraged. Microshare is dedicated to collaborating with independent security researchers to address potential security vulnerabilities.

For research into our services, helpful resources include our Microshare documentation and company website.

Please review these terms before testing or reporting a vulnerability.

Scope

Microshare encourages the responsible discovery and reporting of security vulnerabilities. The following conduct is out of the scope of Microshare's Security Vulnerability Disclosure Policy. Performing any of the following activities is expressly prohibited:

- Actions that might negatively affect Microshare or its users (Brute Force, Denial of Service…)
- Targeting assets of Microshare customers
- Any vulnerability discovered through the compromise of Microshare employee or Microshare customer accounts
- Physical or electronic attacks against Microshare employees or offices
- Social engineering of Microshare employees, contractors, vendors, or service providers
- Knowingly posting, transmitting, linking to, uploading, or sending malware
- Pursuing vulnerabilities that distribute spam
- Violating any laws or breaching any agreements to discover vulnerabilities

Reporting

Microshare encourages the prompt reporting of potential security vulnerabilities. Discoveries that could impact Microshare or our users should be reported as soon as possible. Legitimate reports will be investigated. Subsequent actions to resolve the issue will be conducted in a timely manner. Please follow Microshare's Security

Vulnerability Disclosure Policy and make a good faith effort to avoid privacy violations, interruption or degradation of our service, and data destruction while researching.

If you would like to report a vulnerability or have a security concern, please email support@microshare.io.

Recommended Report Format

Microshare strongly encourages the submission of high-quality vulnerability reports. Reports that are unclear, or do not meet the required level of quality will not be evaluated. To ensure quality, please include the following pieces of information when submitting a report. Doing so will ensure the report is readable and contains the necessary information.

- Affected target, feature, or URL:
- Description of problem:
- Impact of the issue:
- Steps to reproduce:
- Proof of Concept:
- Is knowledge of this issue currently public?

Preferences

Please do not share information regarding unresolved vulnerabilities with third parties. Microshare will make reasonable efforts to respond to reports in a timely manner. Accepted reports will be responded to with an acknowledgment receipt. We will make reasonable efforts to provide an estimated time frame for addressing the vulnerability and notify you when a resolution has been reached.

Microshare appreciates the efforts of every independent security researcher who submits a vulnerability report. We thank you for your help towards enhancing our security posture.