MENDAERA™

MENDAERA INC.
VULNERABILITY DISCLOSURE POLICY

Last Updated: May 17th, 2024

At Mendaera, safeguarding the security of our systems and information is paramount. This policy serves to provide clear guidelines for security researchers engaging in vulnerability discovery activities and outlines our preferred procedures for reporting any discovered vulnerabilities.

Commitment to Collaboration

We value and appreciate the efforts of security researchers in assisting us to maintain the integrity of our systems. Should you make a good faith effort to adhere to this policy during your security research, we will recognize your work as authorized. In such cases, we pledge to collaborate with you to promptly understand and resolve any identified issues. Additionally, we assure you that we will not pursue legal action relating to your research.

Guidelines

Under this policy, "research" refers to activities wherein you:

- Notify us promptly upon discovering any real or potential security issues.
- Make every endeavor to avoid privacy violations, user experience degradation, system disruption, or data manipulation or destruction.
- Use exploits solely to confirm the presence of vulnerabilities. Do not exploit them to compromise or extract data, establish persistent access, or pivot to other systems.
- Allow us a reasonable timeframe to address the issue before further disclosure.
- Refrain from submitting a high volume of low-quality reports.

Should you identify a vulnerability or encounter sensitive data (including personally identifiable information, financial details, or proprietary information), cease testing immediately, notify us immediately, and refrain from disclosing this data to any other party.

Test methods

The following test methods are not permitted:

- Network denial of service (DoS or DDoS) tests or any other actions that impair system access or data integrity.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

Scope

This policy applies to all Mendaera domains including website and internet-accessible product components listed below:

- mendaera.com
- *.mendaera.com
- avail.io
- *.avail.io

Reporting a vulnerability

Information submitted under this policy will solely be used for defensive purposes – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely Mendaera's*, we may share your report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. Your name and contact information will not be shared without your express consent.*

Vulnerability reports can be submitted via security@mendaera.com and may be done so anonymously. If contact information is provided, we aim to acknowledge receipt of your report within 5 business days.

What we expect from you

To assist us in triaging and prioritizing submissions, we recommend that your reports:

- Describe where the vulnerability was discovered and the potential impact of exploitation.
- Provide a detailed account of the steps necessary to reproduce the vulnerability (proof of concept scripts or screenshots are beneficial).
- Be written in English, if possible.

What you can expect from us

When you opt to share your contact information:

We commit to acknowledging receipt of your report within 5 business days.

- We will endeavor to confirm the existence of the vulnerability and maintain transparency regarding the remediation process, including any issues or delays.
- An open dialogue will be maintained to address any concerns or queries you may have.