Responsible vulnerability disclosure

About:

Io.Net is a decentralized network built on Solana that pools spare GPU computing power from various sources, including data centers and crypto miners. This makes it a boon for AI and ML teams looking for cost-effective computing resources.
It offers a platform that leverages large but underutilized global GPU reserves to execute complex tasks such as parallel training and hyperparameter tuning over a distributed network.
At its core, io.net offers a binary token system called $IO and $IOSD to reward participants for network support and task execution. Although the mechanisms of $IO token mining are not publicly disclosed, $IOSD tokens compensate providers for their uptime and performance by combining incentives with innovation.
This model not only democratizes access to high-power computing, but also takes a significant step towards a decentralized computing future. It paves the way for a more efficient and scalable approach to meet the evolving needs of the AI research field, instilling confidence in its future-proofing capabilities.

Policy:

At Io.Net, the security of our users is our number one priority. As such, we strive to provide the most secure platform possible. We will evaluate reported security issues based on the security impact on our users and the Io.Net ecosystem. This bounty brief describes the rules of the Io.Net bug bounty program, including the eligibility of vulnerabilities and the rewards.

Rewards/Ratings:

This program uses the Bugcrowd Vulnerability Rating Taxonomy to prioritize/rate findings. However, prioritization/ratings may vary from the Bugcrowd Vulnerability Rating Taxonomy.

Rewards will be paid in IO.

Once your submission is accepted, please provide your Solana wallet address so you can receive your reward.

*Prices will change with the cryptocurrency markets, and the dollar amount listed below could change.

Please note that only Business critical vulnerabilities with a working proof of concept showing how they can be exploited will be considered eligible for monetary rewards. Io.Net determines whether a reported issue sufficiently meets the bar for monetary rewards.

*Io.Net is eager to work with the community to ensure that every researcher's finding is rewarded fairly - based on the vulnerability's impact on business and overall severity

Io.Net may award an additional reward bonus for exceptional reports. This will be done at Io.Net’s discretion.

Scope and Rewards

P1 –$3000-$5000, **P2** - $1000-$3000, **P3** - $400-$1000, **P4** - $100-$400

In Scope

- *.io.net
- *.io.solutions
- *.io.systems
- *.iog.org
- Io.Net worker client

Out of Scope

- *.bc8.ai
- *.antbit.io

Actions to avoid:

- Testing on accounts other than those that you own
- Automated testing using tools such as scanners
- Excessive request attempts that affect the availability of our services to all users
- Destruction of data

Ineligible issues (Will be closed as out of scope):

- Theoretical vulnerabilities without actual proof of concept
- Email verification deficiencies, expiration of password reset links, and password complexity policies
- Invalid or missing SPF (Sender Policy Framework) records (incomplete or missing SPF/DKIM/DMARC)
- Clickjacking/UI redressing with minimal security impact
- Email or mobile enumeration (E.g., the ability to identify emails via password reset)
- Information disclosure with minimal security impact (E.g., stack traces, path disclosure, directory listings, logs)
- Internally known issues, duplicate issues, or issues that have already been made public
- Tab-nabbing
- Self-XSS
- Vulnerabilities only exploitable on out-of-date browsers or platforms
- Vulnerabilities related to auto-fill web forms
- Use of known vulnerable libraries without actual proof of concept
- Lack of security flags in cookies
- Issues related to unsafe SSL/TLS cipher suites or protocol version
- Content spoofing
- Cache-control related issues
- Exposure of internal IP addresses or domains
- Missing security headers that do not lead to direct exploitation
- CSRF with negligible security impact (E.g., adding to favorites, adding to cart, subscribing to a noncritical feature)
- Vulnerabilities that require root/jailbreak
- Vulnerabilities that require physical access to a user's device
- Issues that have no security impact (E.g., Failure to load a web page)
- Assets that do not belong to Io.Net
- Any activity (like DoS/DDoS) that disrupts our services
- Installation Path Permissions
- Reports from automated tools or scans
- Links to invalid/expired pages (Only valid if you can demonstrate an actual takeover of an official Io.Net social media account linked to every page, not just specific past announcements/blog posts)
- Social Engineering