Security

At ixo, we highly value security. Learn about how we deal with security and vulnerability reports below.

If you find a security issue, you can contact our team directly at security@ixo.world.

Vulnerabilities

Security researchers and white hat hackers are a vital part of building strong, resilient cryptocurrency protocols. At ixo, we actively support the work that hackers and researchers do to find, report and patch security vulnerabilities.

Coordinated Vulnerability Disclosure Policy

We ask security researchers to keep vulnerabilities and communications around vulnerability submissions private and confidential until a patch is developed to protect the people using the ixo protocols. In addition to this, we ask that you:

- Allow us a reasonable amount of time to correct or address security vulnerabilities.
- Avoid exploiting any vulnerabilities that you discover.
- Demonstrate good faith by not disrupting or degrading the ixo data or services.

Vulnerability Disclosure Process

Once we receive a vulnerability report, ixo will take these steps to address it:

1. ixo will confirm receipt of the vulnerability report within 2 business days. The timing of our response may depend on when a report is submitted. As our daily operations are distributed in time zones across the globe, response times may vary. If you have not received a response to a vulnerability report from us within 2 business days, we encourage you to follow up with us again for a response.
2. ixo will investigate and validate the security issue submitted to us as quickly as we can, usually within 5 business days of receipt. Submitting a thorough report with clear steps to recreate the vulnerability and/or a proof-of-concept will move the process along in a timely manner.
3. ixo will acknowledge the bug, and make the necessary code changes to patch it. Some issues may require more time than others to patch, but we will strive to patch each vulnerability as quickly as our resources and development process allow.
4. ixo will publicly release the security patch for the vulnerability, and acknowledge the security fix in the release notes once the issue has been resolved. Public release

notes can reference to the person or people who reported the vulnerability, unless they wish to stay anonymous.

Contact Us

If you find a security issue, you can contact our team directly at security@ixo.world.

To report the issue through a PGP-encrypted email, here is our pubkey fingerprint: BB2A 81D1 CF91 DF00

https://keys.mailvelope.com/pks/lookup?op=get&search=0xBB2A81D1CF91DF00