Beosin has discovered a vulnerability in the Circom verification library, identified as CVE-2023–33252

Beosin · Follow
2 min read · 1 day ago

Listen Share

BEOSIN
Blockchain Security
Beosin has discovered a vulnerability in the Circom verification library, identified as CVE-2023–33252

Beosin has discovered a vulnerability in the Circom verification library, identified as CVE-2023–33252, and warns the ZK project team to be mindful of the associated risks.

Circom is a Rust-based compiler for zero-knowledge proof circuits. The team behind it also developed the SnarkJS library, which enables the implementation of proof systems, including trusted setups, proof generation, and verification, supporting algorithms such as Groth16, PLONK, and FFLONK.

Previously, Beosin security researchers discovered a severe vulnerability in versions of the SnarkJS library up to and including 0.6.11. This vulnerability allowed attackers to forge multiple proofs that would pass verification, enabling double-spending attacks.

Beosin promptly reported the vulnerability, contacted the project team, and assisted in fixing it. The vulnerability has now been patched. Beosin advises all ZK projects using the SnarkJS library to update to version 0.7.0 to ensure security.

Furthermore, Beosin's security team advises ZK project teams to thoroughly consider the algorithm design and the security risks that may arise from language-specific code implementation when conducting proof verification. Beosin has submitted the vulnerability to the Common Vulnerabilities and Exposures (CVE) disclosure platform and received recognition. (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33252)

Contact

If you have need any blockchain security services, please contact us:

Website **Official Twitter** **Alert** **Telegram** **LinkedIn**