FYEO

Banger

Security Review Update: Dec 20, 2024

Version 1.0

Reviewer: thomas@gofyeo.com

Banger Security Review Update

New security issues, 0

After the development team implemented the latest updates, FYEO conducted a review of the modifications. The primary goal of this evaluation was to ensure the continued robustness of the program's security features, safeguarding user funds and maintaining the overall integrity of the program. The provided changes indicate several key updates and improvements across the program.

Security Improvements

- **Replaced Hardcoded `pool.admin` Comparisons with `ADMIN_PUBKEY`:**
  - Replacing `pool.admin` checks with `ADMIN_PUBKEY` adds clarity and prevents accidental misconfiguration in the contract.
- **Enhanced Arithmetic Safety**
  - **Use of `sum_of_squares` Utility Function:**
    - Introduced `sum_of_squares` for calculations. This function factors numbers and includes overflow checks, which enhance arithmetic safety.
    - Shifting from straightforward multiplication and division to this more robust approach reduces potential errors or vulnerabilities caused by large number calculations.
- **Replaced `scalar` with `10^24`:**
  - Previous implementations relied on `2 * 10^12` as a scalar, which may have been insufficient for precision in certain cases.
- **Introduction of `utils.rs`:**
  - Extracting utility functions like `sum_of_squares` to a dedicated module (`utils.rs`) promotes modularity and reusability. This also makes the code easier to maintain and test independently.

Commit Hash Reference:

For transparency and reference, the security review was conducted on the specific commit hash for the Banger repository. The commit hash for the reviewed versions is as follows:

3556a77780d69142bf0af9297d3185ac4e1df000

Conclusion:

In conclusion, the security aspects of the Banger program remain robust and unaffected by the recent updates. Users can confidently interact with the protocol, assured that their funds are well-protected. The commitment to security exhibited by the development team is commendable, and we appreciate the ongoing efforts to prioritize the safeguarding of user assets.