F Y E O

Turbine

Repo: https://github.com/3uild-3thos/govcontract/

Security Review Update: December 4, 2025

Reviewer: balthasar@gofyeo.com

Security Code Review of Solana Staker Vote Override

New security issues, 1

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.

General Updates:

The update tightens and clarifies the protocol's configuration and stored proposal data, trimming some previously permissive defaults and adding explicit timing parameters for discussion, voting, and snapshot behavior. Several compile-time conditional variants were removed in favor of single, consistent values (for things like minimum stake and multipliers), and new constants were introduced to define how long different phases last. Proposal records were expanded to hold additional metadata (including a seed and the vote account identity) and a default initialization was added so new records start in a consistent state. A small utility for converting epoch numbers into slot ranges was also added to support the new time/slot calculations.

Operationally, the code now performs stricter validation and safer account handling around voting and overrides, and it changes how delegator overrides are tracked and applied so cached data is created and updated more robustly. The flow that moves a proposal from support to active voting was adjusted so snapshot selection, consensus linkage, and ballot-box setup happen more deterministically and are explicitly initialized when the activation threshold is met (and there's also a new explicit operation to refresh the snapshot/consensus). Overall the changes aim to reduce ambiguous or uninitialized state, make on-chain bookkeeping more consistent, and harden the vote/override paths against malformed or missing account data.

Missing Snapshot Slot Initialization & Timestamp/Epoch Emission Inconsistencies

Finding ID: FYEO-GOV-01
Severity: **Informational**
Status: **Remediated**

Description

The `ProposalCreated` event emits fields that do not reflect the actual initialization flow. First, `snapshot_slot` is always emitted as `0` because it is not initialized during proposal creation, making the emitted value misleading. Second, the proposal stores both `creation_epoch` and `creation_timestamp`, but the event emits only the timestamp. This inconsistency may cause confusion for indexers or off-chain consumers expecting both values or consistent epoch information.

Proof of Issue

File name: contract/programs/govcontract/src/instructions/create_proposal.rs
Line number: 101

```
// Emit proposal created event
snapshot_slot: self.proposal.snapshot_slot, // Always 0 at this stage
creation_timestamp: self.proposal.creation_timestamp, // creation_epoch omitted
```

Severity and Impact Summary

The issue does not affect on-chain logic or security, but produces misleading event data and complicates off-chain indexing or analytics relying on snapshot slot or epoch values.

Recommendation

Emit accurate and complete initialization metadata. Ensure consistency between stored fields and emitted fields to avoid ambiguity.

Commit Hash Reference:

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

3a2801e33546bd521efb73093b297919c749478d

Remediations have been submitted with the commit hash: 09d13af9e32319bb126f94bf1fbfca86991efb54.

Conclusion:

In conclusion, the security aspects of the Turbine 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.