Tally Staker Deposit Cap Review

February 6, 2025

Prepared for DappHero Corp

Conducted by:

Richie Humphrey (devtooligan)

About the Tally Staker Deposit Cap Review

Tally is a blockchain-based governance platform that enables organizations to manage decision-making through transparent, decentralized processes.

Tally developed the Staker contract which allows users to delegate their voting while staking their governance tokens to earn rewards. The subject of this review is the new StakerCapDeposits extension implements a deposit cap mechanism to limit the total amount of tokens that can be staked in the system.

About Offbeat Security

Offbeat Security is a boutique security company providing unique security solutions for complex and novel crypto projects. Our mission is to elevate the blockchain security landscape through invention and collaboration.

Scope

The src/extensions folder of the `staker` repo was reviewed at commit 76b0d6e.

The following **1 contract** was in scope:

- src/extensions/StakerCapDeposits.sol

Analysis and Findings

The StakerCapDeposits extension implements a simple deposit cap mechanism by adding a state variable to track the maximum allowed total stake, a setter function to control this cap, and modifications to the `stake()` and `stakeMore()` functions to enforce the cap limit. The implementation is concise and follows a straightforward approach with minimal complexity, resulting in a very small attack surface.

```
function _revertIfCapExceeded(uint256 _amount) internal view virtual {
  if ((totalStaked + _amount) > totalStakeCap)
    revert StakerCapDeposits__CapExceeded();
 }
```

The code is well-written and follows best practices. The deposit cap functionality is implemented in a clear and secure manner.

No security issues were identified during the review.