Audit Report - Spacebar

Auditor : taek lee

report delivered at : 2024/02/21

About the auditor

Delivering audits as an independent auditor starting at 2022 December, also working as a security researcher at spearbitDAO.

Grantee of ethereum foundation's impact gift for erc4337 security contributions, nominated by yoav weiss, security fellow of ethereum foundation.

Started a career as smart contract security auditor at 2018, delivered audit to 300+ protocols while being the auditor/lead auditor of haechi-labs, including erc20, nft, defi protocols.

Table of contents

Methods used

- Manual testing using foundry
- Fuzz testing and invariant testing using foundry and halmos

Audited Files

github link :

- https://github.com/ao-labs/blast-spacebar-contract
- https://github.com/ao-labs/blast-staking-contract

commit hash :

- blast-spacebar-contract : 5200600
- blast-staking-contract : 40209db

Update Commit Log

1.0 :

- blast-spacebar-contract : 5200600
- blast-staking-contract : 40209db

Summary

Severity	Title	Status
Minor	Staking contract uses <address>.transfer to withdraw	Found - v1.0
Minor	Operator can choose starting/end price	Found - v1.0

Issues

[Minor] Staking contract uses <address>.transfer to withdraw

On staking contract, withdraw function is used to withdraw the stake amount to the specified address. Since registry passes the msg.sender of the caller which is the owner of the staking contract, it will transfer the eth staked into the staking contract back to the owner.\
While doing that, Staking contract uses <address>.transfer to transfer the native token. BUT, transfer function has stipend gas limit of 2300, which makes it impossible to receive fund if the recipient is smart contract.
This issue will not affect any EOA, or if the smart contract account has `receive()` function that does not use much gas

Recommendation

Avoid using the staking registry with smart contract, if there are use cases where smart contract needs to interact with the staking registry, consider using `<address>.call{value:amount}()` to make sure it won't fail.

[Minor] Staking Registry's before/after hook will be ignored when hook recipient fails

Staking registry utilizes hook design to make it flexible for service to receive the deposit/withdraw data. But staking registry does not revert on hook failure. So if you are building a service that relies on the hook to track the data, make sure hook does not fail on any cases.

Recommendation

- Avoid building hook that can fail.
- Modify the registry code to revert the tx when hook has failed