Dappd Audit Summary

Project: FarmerDoge
August 12, 2022

Contents

Disclaimer

Project Summary

Farmerdoge is a multi dividend rewards token. Our contract allows us to switch our rewards token. Every month we provide the community with 5 BSC projects to read up on, we do our own research prior and provide a brief write up and links for the community to look into.

5 days later we provide a DAO for CROP holders to take part in a vote to choose 1 project to be the rewards token for the next month.

We are also a charitable project, with plans to create partnerships with with real world farmers and food suppliers to help with food waste and food distribution

Contracts Audited

- FarmerDoge Token
  - 0x288F7692a78aA9906Cf5790aF78a672078070535
- DividendTracker
  - 0xd7C6f5b674Ef7A48164C24df56700c1D71CE1C60

Audit Results

PASSED

Critical Issues

No Issue

High Issues

#	File	Line	Issue
1	FarmerDoge Token	859-992	Centralization Risks

Medium Issues

No Issue

Low Issues

#	File	Line	Issue
1	FarmerDoge Token	1087-1088	setBalance Call Error Should Not Be Caught

Misc Issues

#	File	Line	Issue
1	FarmerDoge Token	429, 466, 606, 818, 1219	Compiler Warnings
2	FarmerDoge Token	685	Logic Is Ignored
3	Dividend Tracker	1230	Compiler Warnings
4	Dividend Tracker	1355	Gas Optimization

Descriptions and Mitigation

Note: The purpose of this section is to add further clarity for any findings, as well as offer a proposed mitigation for these findings. These proposals are meant to be taken as suggestions or advice.

High Issues

Issue #1

#	File	Line	Issue
1	FarmerDoge Token	859-992	Centralization Risks

Description

- Contract owner is able to set the fees for buying and selling to any value, including 100%, this could result in the token contract becoming a honeypot, where investors are able to buy the token, but only selected investors can sell the token
- Contract owner is able to disable and enable trading of the token for certain accounts at will
- Contract owner is able to set the maximum holdings of certain wallets to any value, including 0
- Contract owner is able to set the max transaction amount of certain wallets to any value, including 0
- Contract owner is able to set the reward token and uniswap router, allowing them to siphon tokens that were supposed to be given as rewards

Mitigation

- Have a maximum upper threshold in place to prevent the buy and sell fee from ever reaching a constant specified limit I.E. 50% or 100%
- Create an owner contract to call owner functions on behalf of an existing owner, and hardcode limitations into the owner contract itself to avoid abuse

Low Issues

Issue #1

#	File	Line	Issue
1	FarmerDoge Token	1087-1088	setBalance Call Error Should Not Be Caught

Description

The setBalance function is put inside of a try catch block. This function is what tells the DividendTracker the balance of particular users so that it may allocate new rewards to the correct users. If this function errors or runs out of gas, a user could continue to gain rewards even after selling out their balance, or receive less rewards than they should. This function is critical to the functionality of the token, so it should not be placed inside of a try catch block, instead error handling should be performed inside of the setBalance function itself, as its execution succeeding is paramount to the logic of the system.

Mitigation

Remove this try catch block, as the logic inside of setBalance is crucial to execute and if it throws an error, that error should not be ignored.

Misc Issues

Issue #1

#	File	Line	Issue
1	FarmerDoge Token	429, 466, 606, 818, 1219	Compiler Warnings

Description

Constructor visibility is ignored

Continue...

. . . Continue

Mitigation

Delete the public keyword

Issue #2

#	File	Line	Issue
2	FarmerDoge Token	685	Logic Is Ignored

Description

require false inside this function will make all logic written underneath never execute.

Mitigation

These lines should be removed

Issue #3

#	File	Line	Issue
3	Dividend Tracker	1230	Compiler Warnings

Description

Function can be scoped to pure

Mitigation

Scope function to pure

Issue #4

Continue. . .

. . . Continue

#	File	Line	Issue
4	Dividend Tracker	1355	Gas Optimization

Description

Unnecessary gas spent on redundant logic.

Mitigation

processAccount() should be scoped to internal and the onlyOwner modifier removed.
Since the token does not call this function itself, and rather it is called from other functions which are already scoped to onlyOwner, this check is redundant and adds O(n) gas for every dividend distributed in setBalance and process