Audit of the YFValue Version 2 Staking Pool

a report authored by

Minh Khai Do

Summaries by

Rasikh Morani

Joel Farris

innovative fortuna iuvat

1 September, 2020

0.1 Executive Summary

A Representative Party of the YFValue Decentralized Organization ("YFValue") engaged The Arcadia Group ("Arcadia"), a software development, research and security company, to conduct a review of the YFValue Smart Contract YFV$_S take_V 2.sol("YFVStake")$

Arcadia completed the review using various methods primarily consisting of dynamic and static analysis. The assessment identified a small amount of issues, soley in the area of low level descriptions.

0.2 Recommendations Summary

0.2.1 Short Term

- Remediate all known findings
- Implement scaling deposit and daily volume limits to de-risk smart contracts, alternatively, break larger pools into multiple contracts to spread holdings across multiple contracts

Findings

Dynamic Findings

Severity:

Notice

Type:

Dynamic

Lines:

38, 70, 229, 260, 338, 424, 495, 572, 587

Description:

The Contract does not use the same solidity version uniformly across the contract, which may lead to compatibility issues and potentially future pipeline issues.

Severity:

Notice

Type:

Dynamic

Lines:

815-825, 782-792

Description:

Increase code clarity using comments covering logic behind conditional staking amount and deposit fee rules.

Severity:

Optimization

Type:

Dynamic

Lines:

870-881

Description:

In the function getReward, the rewards amount is updated using the updateReward modifier, it is later re-calculated by calling the earned function. This can be optimized by modifying to avoid re-calculation.

Static Findings

Severity:

Low-Code Optimization

Contract:

All Contracts

Type:

Static

Description:

YFV utilizes a floating pragma, which is not recommended per SWC-103, which recommends utilizing a fixed pragma to avoid potential introduced issues, and so the bytecode does not vary between builds.