Smart Contract Audit for Forthewin

Overlord Security

April 22, 2023

Contents

1 Project Overview

Created by: ForTheWin

Based on: Ethereum

Date Conducted: April, 2023

ForTheWin

Contracts: **FTWSwap**
Github: `https://github.com/ForTheWinn/FTW-Solidity-Contracts/tree/main/contracts`
Commit: **908a0b5**
Programming Language: **Solidity**
Development Env: **solidity** $\wedge$ **0.8.0**

2 Project Introduction

Forthewin ecosystem will create a platform where ordinary users and businesses can easily use both Fungible tokens and NFTs in their daily lives and find more use cases. The motivation is to give everyone the opportunity to create and manage both Fungible tokens and NFTs, help them be successful and allow their tokens to be more heavily adopted into every day life.

3 Findings and Recommendations

3.1 Summary

The following findings and recommendations after analyzing the **FortheWin Swap contract** implementation. Any additional recommendations beyond what any scanning tools supply are included as necessary.

Severity	Number of findings
Critical	0
Medium	0
Low	2
Informational	4

Issue Id	Severity	Title	Category	Fixed
MS-01	Informative	Typo in Function call	Typo	Fixed
MS-02	Low	Lack of inputs validation	Business logic	Fixed
MS-03	Low	Lack of inputs validation	Business logic	Fixed
MS-04	Informative	Redundant comparison	Coding Practices	Fixed
MS-05	Informative	Typo	Coding Practices	Fixed
MS-06	Informative	Unnecessary external call	Optimization	Fixed

3.2 Low Vulnerabilities

MS-02: Lack Inputs of Validation
Lack Inputs of Validation
Source Code link
https://github.com/ForTheWinn/FTW-Solidity-Contracts/blob/bfbbd191c9f26314fbc4df988655b7c1f757ec4e/contracts/FTWSwap/FTWSwap.sol#L91
Description
It is recommended to check that the amount of tokens being added is not zero.
Solution
The zero check can be added at the beginning of the function.
Status
The issue has been confirmed by team and fixed in commit `310da05`

MS-03: Lack Inputs of Validation

Lack Inputs of Validation

Source Code link

https://github.com/ForTheWinn/FTW-Solidity-Contracts/blob/bfbbd191c9f26314fbc4df988655b7c1f757ec4e/contracts/FTWSwap/FTWSwap.sol#L94

Description

The code checks that the two tokens are not the same, which is good. However, it does not check that the tokens are valid ERC20 tokens. It is recommended to add a check for this.

Solution

Change to something like require(isValidERC20(tokenA) isValid-ERC20(tokenB), "Invalid ERC20 token.");

Status

The issue has been confirmed by team and fixed in commit `e3c019a`

3.3 Informational Vulnerabilities

MS-01: Typo in function call

Typo in function call

Source Code link

https://github.com/ForTheWinn/FTW-Solidity-Contracts/blob/bfbbd191c9f26314fbc4df988655b7c1f757ec4e/contracts/FTWSwap/FTWSwap.sol#L294

Description

The function withdraws the output token from the contract's address to the user's address using _safeWidthdraw(). However, the function name seems to have a typo as "withdraw" is spelled as "widthdraw". This should be corrected.

Solution

It is recommended to fix the typo to avoid further ambiguous mistakes.

Status

The issue has been confirmed by the team and fixed in commit `41b00b0`

MS-04: Redundant comparison

Redundant comparison

Source Code link

https://github.com/ForTheWinn/FTW-Solidity-Contracts/blob/bfbbd191c9f26314fbc4df988655b7c1f757ec4e/contracts/FTWSwap/FTWSwap.sol#L100

Description

The compare to true is not necessary.

Solution

Can be modified as if (reserves.createdAt)

Status

The issue has been confirmed by the team and fixed in commit `a25b1fb`

MS-05: Typo

Typo

Source Code link

https://github.com/ForTheWinn/FTW-Solidity-Contracts/blob/bfbbd191c9f26314fbc4df988655b7c1f757ec4e/contracts/FTWSwap/FTWSwap.sol#L464

Description

There is a typo.

Solution

Can be modified as require(fee > 0, "fee is out of range.");

Status

The issue has been confirmed by the team and fixed in commit `6713987`

MS-06: Unnecessary external call

Unnecessary external call

Source Code link

https://github.com/ForTheWinn/FTW-Solidity-Contracts/blob/bfbbd191c9f26314fbc4df988655b7c1f757ec4e/contracts/FTWSwap/FTWSwap.sol#L4

Description

it's better to use an internal call instead of an external call for this erc721-safe-transfer

Solution

directly call safeTransferFrom

Status

The issue has been confirmed by the team and fixed in commit `52c8a02`

4 Conclusion

In this audit, we have analyzed the **Forthewin Swap contract** design and implementation. The current code base is well organized and those identified issues are promptly confirmed and fixed.

Meanwhile, we need to emphasize that smart contracts as a whole are still in an early, but active stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

For more information regarding this audit report, please send email to contact@overlord.wtf