PALADIN
BLOCKCHAIN SECURITY

# Smart Contract Security Assessment

Final Report

## For ApeSwap (Zap)

03 May 2023

paladinsec.co

info@paladinsec.co

# Table of Contents

# Disclaimer

Paladin Blockchain Security ("Paladin") has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies. Further, this audit report shall not be disclosed nor transmitted to any persons or parties on any objective, goal or justification without due written assent, acquiescence or approval by Paladin.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Paladin is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Paladin or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

Cryptocurrencies and any technologies by extension directly or indirectly related to cryptocurrencies are highly volatile and speculative by nature. All reasonable due diligence and safeguards may yet be insufficient, and users should exercise considerable caution when participating in any shape or form in this nascent industry.

The audit report has made all reasonable attempts to provide clear and articulate recommendations to the Project team with respect to the rectification, amendment and/or revision of any highlighted issues, vulnerabilities or exploits within the contracts provided. It is the sole responsibility of the Project team to sufficiently test and perform checks, ensuring that the contracts are functioning as intended, specifically that the functions therein contained within said contracts have the desired intended effects, functionalities and outcomes of the Project team.

Paladin retains full rights over all intellectual property (including expertise and new attack or exploit vectors) discovered during the audit process. Paladin is therefore allowed and expected to re-use this knowledge in subsequent audits and to inform existing projects that may have similar vulnerabilities. Paladin may, at its discretion, claim bug bounties from third-parties while doing so.

# 1 Overview

This report has been prepared for ApeSwap's Zapper contracts on the BNB Smart Chain. Paladin provides a user-centred examination of the smart contracts to look for vulnerabilities, logic errors or other issues from both an internal and external perspective.

## 1.1 Summary

| | |
|---|---|
| **Project Name** | ApeSwap (Zap contracts) |
| **URL** | https://apeswap.finance |
| **Network** | BNB Smart Chain |
| **Language** | Solidity |
| **Preliminary** | https://github.com/ApeSwapFinance/apeswap-hardhat-zap/tree/d7980fb159f387f0e844f6a93c517bb9c3bc4ecd/contracts |
| **Resolution** | https://github.com/ApeSwapFinance/apeswap-hardhat-zap/pull/2/commits/c68adaefaeca6fe90c7446b8257a2c584486b444 |

## 1.2 Contracts Assessed

| Name | Contract | Live Code Match |
| --- | --- | --- |
| ApeSwapZap | | |
| ApeSwapZapExtendedV0 | | |
| TransferHelper | | |
| ApeSwapZapMiniApeV2 | | |
| ApeSwapZapMasterApeV2 | | |
| ApeSwapZapLending | | |
| ApeSwapZapVaults | | |
| ApeSwapZapPools | | |
| ApeSwapZapLPMigrator | | |
| ApeSwapZapTBills | | |

## 1.3 Findings Summary

| Severity | Found | Resolved | Partially Resolved | Acknowledged (no change made) |
|---|---|---|---|---|
| High | 0 | - | - | - |
| Medium | 0 | - | - | - |
| Low | 0 | - | - | - |
| Informational | 3 | 3 | - | - |
| **Total** | **3** | **3** | **-** | **-** |

### Classification of Issues

| Severity | Description |
|---|---|
| High | Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency. |
| Medium | Bugs or issues that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible. |
| Low | Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless. |
| Informational | Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any. |

### 1.3.1 ApeSwapZap

| ID | Severity | Summary | Status |
|---|---|---|---|
| 01 | INFO | Typographical issue | ✓ RESOLVED |

### 1.3.2 ApeSwapZapExtendedV0

No issues found.

### 1.3.3 TransferHelper

No issues found.

### 1.3.4 ApeSwapZapMiniApeV2

| ID | Severity | Summary | Status |
|---|---|---|---|
| 02 | INFO | Typographical issue | ✓ RESOLVED |

### 1.3.5 ApeSwapZapMasterApeV2

No issues found.

### 1.3.6 ApeSwapZapLending

No issues found.

### 1.3.7 ApeSwapZapVaults

No issues found.

### 1.3.8 ApeSwapZapPools

No issues found.

### 1.3.9 ApeSwapZapLPMigrator

No issues found.

### 1.3.10 ApeSwapZapTBills

| ID | Severity | Summary | Status |
|---|---|---|---|
| 03 | INFO | Typographical issue | ✓ RESOLVED |

# 2 Findings

## 2.1 ApeSwapZap

`ApeSwapZap` is an abstract contract that allows users to exchange (zap) tokens or native assets (e.g. BNB) into an LP within a single function call. It receives an amount of token X and zaps it into a minimum amount of tokens Y-Z LP.

Additionally, it can zap a native token, e.g. BNB, into an LP by wrapping it. If the minimum amount that was zapped is lower than the amount sent by the user, the contract refunds the rest into the tokens that the LP is created from.

### 2.1.1 Issues & Recommendations

| Issue #01 | Typographical issue |
|---|---|
| **Severity** | INFORMATIONAL |
| **Description** | Line 238<br>`ApeSwapZap: path0 is required for this operation`<br><br>Replace path0 with path1. |
| **Recommendation** | Consider resolving the typographical issue. |
| **Resolution** | RESOLVED |

## 2.2 ApeSwapZapExtendedV0

`ApeSwapZapExtendedV0` implements the `ApeSwapZapTBills`, `ApeSwapZapMasterApeV2` and `ApeSwapZapLending` into one contract.

### 2.2.1 Issues & Recommendations

No issues found.

## 2.3 TransferHelper

`TransferHelper` is a contract to transfer in/out tokens from and into the contract.

### 2.3.1 Issues & Recommendations

No issues found.

## 2.4 ApeSwapZapMiniApeV2

`ApeSwapZapMiniApeV2` is an abstract contract that extends the capabilities of the ApeSwapZap contract by offering to the user the possibility to exchange (zap) single tokens into the dual farms contracts called MiniApeV2.

### 2.4.1 Issues & Recommendations

| Issue #02 | Typographical issue |
|---|---|
| **Severity** | INFORMATIONAL |
| **Description** | Line 116<br>`ApeSwapZap: Wrong LP pair for Dual Farm`<br><br>Replace `ApeSwapZap` with `ApeSwapZapMiniApeV2`. |
| **Recommendation** | Consider resolving the typographical issue. |
| **Resolution** | RESOLVED |

## 2.5 ApeSwapZapMasterApeV2

`ApeSwapZapMasterApeV2` is an abstract contract that extends the capabilities of the `ApeSwapZap` contract by offering to the user the possibility to exchange (zap) single tokens into various farms contracts called MasterApeV2.

### 2.5.1 Issues & Recommendations

No issues found.

## 2.6 ApeSwapZapLending

`ApeSwapZapLending` is an abstract contract that extends the capabilities of the `ApeSwapZap` contract by offering to the user the possibility to exchange (zap) single tokens into a lending market.

### 2.6.1 Issues & Recommendations

No issues found.

## 2.7 ApeSwapZapVaults

`ApeSwapZapVaults` is an abstract contract that extends the capabilities of the `ApeSwapZap` contract by offering to the user the possibility to exchange (zap) single tokens into a lending market.

### 2.7.1 Issues & Recommendations

No issues found.

## 2.8 ApeSwapZapPools

`ApeSwapZapPools` is an abstract contract that extends the capabilities of the ApeSwapZap by allowing a user to exchange (zap) LP tokens and deposit them into ApeSwap pools. The contract also allows users to deposit single assets into BANANA/GNANA pools.

This contract has already been audited by Paladin; the changes applied to them do not reflect additional issues other than the ones resolved already by the team in the previous audit. (https://paladinsec.co/projects/apeswap/)

### 2.8.1 Issues & Recommendations

No issues found.

## 2.9 ApeSwapZapLPMigrator

`ApeSwapZapLPMigrator` is an abstract contrat that offers to the user the possibility to exchange (zap) a non-Ape LPs to APE LPs. It's using a non-APE LP router to swap the liquidity from non-APE LPs into APE-LPs.

This contract has already been audited by Paladin; the changes applied to them do not reflect additional issues other than the ones resolved already by the team in the previous audit. (https://paladinsec.co/projects/apeswap/)

### 2.9.1 Issues & Recommendations

No issues found.

## 2.10 ApeSwapZapTBills

`ApeSwapZapTBills` is an abstract contract that extends the capabilities of the ApeSwapZap by offering to the user the possibility to exchange (zap) single or LP tokens into Treasury Bills in a single operation.

This contract has already been audited by Paladin; the changes applied to them do not reflect additional issues other than the ones resolved already by the team in the previous audit. (https://paladinsec.co/projects/apeswap/)

### 2.10.1 Issues & Recommendations

| Issue #03 | Typographical issue |
|---|---|
| **Severity** | INFORMATIONAL |
| **Description** | Line 198<br>`ApeSwapZap: Wrong LP pair for TBill`<br><br>Replace `ApeSwapZap` with `ApeSwapZapTBills`. |
| **Recommendation** | Consider resolving the typographical issue. |
| **Resolution** | RESOLVED |


PALADIN
BLOCKCHAIN SECURITY