

2 Dec 2022

**DRIVENsecurity**

Premium Audit

**Ark Fi**

Static Code Analysis & Manual  
Verification For Smart Contract

[WWW.DRIVENEcosystem.COM](http://WWW.DRIVENEcosystem.COM)



# Disclaimer

Accepting a project audit can be viewed as a sign of confidence and is typically the first indicator of trust for a project, but it does not guarantee that a team will not remove all liquidity, sell tokens, or engage in any other type of fraud. There is also no method to restrict private sale holders from selling their tokens. It is ultimately your obligation to read through all documentation, social media posts, and contract code for each particular project in order to draw your own conclusions and define your own risk tolerance.

DRIVENlabs Inc. accepts no responsibility for any losses or encourages speculative investments. This audit's material is given solely for information reasons and should not be construed as investment advice.

# Table Of Contents

Project Details .....	3
Static Analysis .....	4
Issues .....	6
Recommendations .....	9
Conclusion .....	10



# Project Details

Name of the project:

Ark Fi

Website:

<https://www.arkfi.io/>

Type of the Smart Contract:

Custom Smart Contract

Chain:

BNB Smart Chain

Address:

0x3333e437546345F8Fd48Aa5cA8E92a77eD4b3333

Explorer Link:

[https://bscscan.com/  
address/0x3333e437546345F8Fd48Aa5cA8E92a77eD4b3333#co  
de](https://bscscan.com/address/0x3333e437546345F8Fd48Aa5cA8E92a77eD4b3333#code)

Website: <https://www.arkfi.io/>



# Static Analysis

SWC ISSUES	STATUS
Function Default Visibility	PASSED
Integer Overflow and Underflow	PASSED
Outdated Compiler Version	PASSED
Floating Pragma	PASSED
Unchecked Call Return Value	PASSED
Unprotected Ether Withdrawal	PASSED
Unprotected SELFDESTRUCT Instruction	PASSED
Reentrancy	HIGH SEVERITY / LOW SEVERITY (SOLVED)
State Variable Default Visibility	PASSED
Uninitialized Storage Pointer	PASSED
Assert Violation	PASSED
Use of Deprecated Solidity Functions	PASSED
Delegatecall to Untrusted Callee	PASSED
DoS with Failed Call	PASSED
Transaction Order Dependence	PASSED
Authorization through tx.origin	PASSED
Block values as a proxy for time	PASSED
Signature Malleability	PASSED
Incorrect Constructor Name	PASSED
Shadowing State Variables	PASSED
Weak Sources of Randomness from Chain Attributes	PASSED
Missing Protection against Signature Replay Attacks	PASSED
Lack of Proper Signature Verification	PASSED
Requirement Violation	PASSED



# Static Analysis

SWC ISSUES	STATUS
Write to Arbitrary Storage Location	PASSED
Incorrect Inheritance Order	PASSED
Insufficient Gas Griefing	PASSED
Arbitrary Jump with Function Type Variable	PASSED
DoS With Block Gas Limit	PASSED
Typographical Error	PASSED
Right-To-Left-Override control character (U+202E)	PASSED
Presence of unused variables	PASSED
Unexpected Ether balance	PASSED
Hash Collisions With Multiple Variable Length Arguments	PASSED
Message call with hardcoded gas amount	PASSED
Code With No Effects	PASSED



# Issues

## Static Code Analysis

No major issues were found.

## Manual Verification

### Compilation Errors:

- Undeclared events/variables:

```
emit RewardsCompounded(investor, claimableNow);
emit BondTaxesTaken(instantRewards, poolRewards, treasuryAmount);
bondTax variable;

>>> uint256 taxAmount = amount * bondTax / 100;
>>> uint256 instantRewards = amount * instantPercent / bondTax;
>>> uint256 poolRewards = amount * poolPercent / bondTax;
```







# Recommendations

- The “rescueAnyToken” can be re-written like this:

```
function rescueAnyToken(IBEP20 tokenToRescue) external  
onlyCEO {  
    uint256 _balance = tokenToRescue.balanceOf(address(this));  
    tokenToRescue.transfer(msg.sender, _balance);  
}
```

- Add a “require” statement for BUSD transfers in the following functions: “sendRewards”, “\_claim”, “addToRewardsPool”.

```
BUSD.transferFrom(msg.sender, address(this), busdAmount);
```

TO

```
require(BUSD.transferFrom(msg.sender, address(this),  
busdAmount), "Failed!");
```



# Conclusion

Done: The Ark Fi team is aware of our findings.

*Done [06 Dec. 2022]: Solve the issues.*

*Update [17 Dec. 2022]: Issues were solved and the smart contract was deployed.*

2 Dec 2022

**Thank  
you!**