Cyberscope

Audit Report

ETFSwap

April 2024

Repository https://github.com/etfswap/etfswap

Commit fef309e2a20670cdd942baa7dd943df53d837c0e

Audited by © cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	MCM	Misleading Comment Messages	Unresolved
	RAU	Redundant Allocation Usage	Unresolved
	L04	Conformance to Solidity Naming Conventions	Unresolved

Table of Contents

Review

Contract Name	ETFSwap
Repository	https://github.com/etfswap/etfswap
Commit	567fed8444a7134cb84da4985b5d0838a6bd7fc5
Testing Deploy	https://testnet.bscscan.com/address/0xaef811cabc8251dda180bcd5dff1710e1198c355
Symbol	ETFS
Decimals	18
Total Supply	1,000,000,000
Badge Eligibility	Must Fix Criticals

Audit Updates

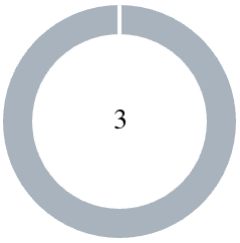
Initial Audit	27 Mar 2024 https://github.com/cyberscope-io/audits/blob/main/etfswap/v1/audit.pdf
Corrected Phase 2	04 Apr 2024 https://github.com/cyberscope-io/audits/blob/main/etfswap/v2/audit.pdf
Corrected Phase 3	05 Apr 2024 https://github.com/cyberscope-io/audits/blob/main/etfswap/v3/audit.pdf
Corrected Phase 4	08 Apr 2024 https://github.com/cyberscope-io/audits/blob/main/etfswap/v4/audit.pdf

Corrected Phase 5	10 Apr 2024 https://github.com/cyberscope-io/audits/blob/main/etfswap/v5/audit.pdf
Corrected Phase 6	16 Apr 2024 https://github.com/cyberscope-io/audits/blob/main/etfswap/v6/audit.pdf
Corrected Phase 7	18 Apr 2024

Source Files

Filename	SHA256
contracts/IERC20.sol	6aea8332bcc2b6f92e6abcb6e1327cd050365452de160e4831e849a995087aac
contracts/ETFSwap.sol	9e166524ae50c6708ecf3480d5df4152144a3022eec20cdcd777a05a67823e87

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	3

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	3	0	0	0

MCM - Misleading Comment Messages

Criticality	Minor / Informative
Location	contracts/ETFSwap.sol#L182
Status	Unresolved

Description

The contract is using misleading comment messages. These comment messages do not accurately reflect the actual implementation, making it difficult to understand the source code. As a result, the users will not comprehend the source code's actual implementation.

```
if (from == liquidityPairAddress) {
    // Apply buy tax rate if the tokens are being transferred
by the owner
    return (tokens * buyTaxRate) / (100);
```

Recommendation

The team is advised to carefully review the comment in order to reflect the actual implementation. To improve code readability, the team should use more specific and descriptive comment messages.

RAU - Redundant Allocation Usage

Criticality	Minor / Informative
Location	contracts/ETFSwap.sol#L52
Status	Unresolved

Description

The contract is designed to mint initial tokens by crediting multiple allocations to the msg.sender's balance. These include `PRESALE_ALLOCATION`, `ECOSYSTEM_ALLOCATION`, `LIQUIDITY_ALLOCATION`, `CASHBACK_ALLOCATION`, `PARTNERS_ALLOCATION`, `COMMUNITY_REWARDS_ALLOCATION`, `MM_ALLOCATION`, and `TEAM_ALLOCATION`. Despite these varied allocations, the contract fails to implement any distinct functionality or checks specific to each allocation type. This leads to a scenario where the different allocation constants essentially serve no unique purpose, causing unnecessary redundancy in the contract's logic. The use of multiple allocations without corresponding functional distinctions not only complicates the codebase but also increases the risk of errors and mismanagement in token distribution processes.

```
balances[msg.sender] += PRESALE_ALLOCATION;
balances[msg.sender] += ECOSYSTEM_ALLOCATION;
balances[msg.sender] += LIQUIDITY_ALLOCATION;
balances[msg.sender] += CASHBACK_ALLOCATION;
balances[msg.sender] += PARTNERS_ALLOCATION;
balances[msg.sender] += COMMUNITY_REWARDS_ALLOCATION;
balances[msg.sender] += MM_ALLOCATION;
balances[msg.sender] += TEAM_ALLOCATION;

uint256 TOTAL_TOKENS_TRANSFERRED = PRESALE_ALLOCATION +
    ECOSYSTEM_ALLOCATION +
    LIQUIDITY_ALLOCATION +
    CASHBACK_ALLOCATION +
    PARTNERS_ALLOCATION +
    COMMUNITY_REWARDS_ALLOCATION +
    MM_ALLOCATION +
    TEAM_ALLOCATION;
```

Recommendation

It is recommended to consolidate these multiple allocations into a single allocation framework since the contract does not utilize the assigned allocations distinctly. By defining one comprehensive allocation parameter or simplifying the allocation structure, the contract can reduce complexity and potential overhead associated with maintaining multiple redundant constants. This approach will streamline the initial token distribution mechanism, enhance clarity, and potentially decrease the likelihood of bugs associated with token allocation.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	contracts/ETFSwap.sol#L92
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
address _liquidityPairAddress
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.
Find more information on the Solidity documentation
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
ETFSwap	Implementation			
		Public	✓	-
	totalSupply	Public		-
	balanceOf	Public		-
	setLiquidityPairAddress	External	✓	onlyOwner
	_transferTokens	Internal	✓	
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	calculateTaxAmount	Private		

	setSellTaxRate	External	✓	onlyOwner
	setBuyTaxRate	External	✓	onlyOwner
	renounceOwnership	Public	✓	onlyOwner

Inheritance Graph

Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
ETFSwap
<Constructor>
onlyOwner
totalSupply
balanceOf
setLiquidityPairAddress
transfer
transferFrom
_transferTokens
calculateTaxAmount
increaseAllowance
decreaseAllowance
setSellTaxRate
setBuyTaxRate
renounceOwnership
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom

Summary

ETFSwap contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. ETFSwap is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 25% fees.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io