Cyberscope

Audit Report

Oracle AI

February 2024

Network ETH

Address 0x57B49219614859176Ddb029298486B6c30193Cbd

Audited by © cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	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
	PLPI	Potential Liquidity Provision Inadequacy	Unresolved
	PVC	Price Volatility Concern	Unresolved
	UFP	Unused Function Parameter	Unresolved
	L02	State Variables could be Declared Constant	Unresolved
	L04	Conformance to Solidity Naming Conventions	Unresolved
	L07	Missing Events Arithmetic	Unresolved
	L08	Tautology or Contradiction	Unresolved
	L17	Usage of Solidity Assembly	Unresolved

Table of Contents

Review

Contract Name	Oracle
Compiler Version	v0.8.19+commit.7dd6d404
Optimization	200 runs
Explorer	https://etherscan.io/address/0x57b49219614859176ddb029298486b6c30193cbd
Address	0x57b49219614859176ddb029298486b6c30193cbd
Network	ETH
Symbol	ORACLE
Decimals	18
Total Supply	1,000,000,000
Badge Eligibility	Yes

Audit Updates

Initial Audit	07 Feb 2024 https://github.com/cyberscope-io/audits/blob/main/2-oracle/v1/audit.pdf
Corrected Phase 2	13 Feb 2024 https://github.com/cyberscope-io/audits/blob/main/2-oracle/v2/audit.pdf
Corrected Phase 3	16 Feb 2024 https://github.com/cyberscope-io/audits/blob/main/2-oracle/v3/audit.pdf
Corrected Phase 4	17 Feb 2024

Source Files

Filename	SHA256
contracts/token.sol	7180bca9d649d4929a5d994b0f0fd03ac7eec3d8c14ddebef7f7e22b53db92cf
contracts/lib/IV2Pair.sol	72e4d1f173754ea270e3fbb80e375440e50a4bd75a1654b83d66959b0a2a2bc6
contracts/lib/IRouter02.sol	f377cfd9244dfa9d707118bd71451b5edf8586bbcff343da59fcb034035a0fc5
contracts/lib/IRouter01.sol	13d90aa270f4305a1f70a2eac357b709caacff55d99022138f99f97bcb38cd02
contracts/lib/IFactoryV2.sol	295e59f29cb4b0374666ce6e900db1cb917c7931a5041d8c038b2a240849ef53
contracts/lib/IERC20.sol	11e301dcd4a99fd3fa03e54e6985b4e0b9310465c65e195ad25ec1a48ea2c138

Findings Breakdown

Critical	1
Medium	0
Minor / Informative	8

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	1	0	0	0
Medium	0	0	0	0
Minor / Informative	8	0	0	0

ST - Stops Transactions

Criticality	Critical
Location	contracts/token.sol#L540
Status	Unresolved

Description

The trading initially is disabled and the contract owner has to enable it. The contract owner has to call the `confirmLP` function.

```
if (!tradingEnabled) {
    revert("Trading not yet enabled!");
}
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

  Permanent Solution:
- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

PLPI - Potential Liquidity Provision Inadequacy

Criticality	Minor / Informative
Location	contracts/token.sol#L428
Status	Unresolved

Description

The contract operates under the assumption that liquidity is consistently provided to the pair between the contract's token and the native currency. However, there is a possibility that liquidity is provided to a different pair. This inadequacy in liquidity provision in the main pair could expose the contract to risks. Specifically, during eligible transactions, where the contract attempts to swap tokens with the main pair, a failure may occur if liquidity has been added to a pair other than the primary one. Consequently, transactions triggering the swap functionality will result in a revert.

```
function contractSwap(uint256 contractTokenBalance) internal swapLock {

    TaxPercentages memory taxPercentages = _taxPercentages;

    if (
        _allowances[address(this)][address(dexRouter)] !=
type(uint256).max
    ) {
        _allowances[address(this)][address(dexRouter)] =
type(uint256).max;
    }

    address[] memory path = new address[](2);
    path[0] = address(this);
    path[1] = dexRouter.WETH();

    dexRouter.swapExactTokensForETHSupportingFeeOnTransferTokens(
        contractTokenBalance,
        0,
        path,
        address(this),
        block.timestamp
    );
    ...
}
```

Recommendation

The team is advised to implement a runtime mechanism to check if the pair has adequate liquidity provisions. This feature allows the contract to omit token swaps if the pair does not have adequate liquidity provisions, significantly minimizing the risk of potential failures.

Additionally, the contract could be designed to tolerate potential reverts from the swap functionality, especially when it is a part of the main transfer flow. This can be achieved by executing the contract's token swaps in a non-reversible manner, thereby ensuring a more resilient and predictable operation.

PVC - Price Volatility Concern

Criticality	Minor / Informative
Location	contracts/token.sol#L331,571,583
Status	Unresolved

Description

The contract accumulates tokens from the taxes to swap them for ETH. The variable `swapThreshold` sets a threshold where the contract will trigger the swap functionality. If the variable is set to a big number, then the contract will swap a huge amount of tokens for ETH.

It is important to note that the price of the token representing it, can be highly volatile. This means that the value of a price volatility swap involving Ether could fluctuate significantly at the triggered point, potentially leading to significant price volatility for the parties involved.

```
function setSwapSettings(
    uint256 threshold,
    uint256 thresholdDivisor,
    uint256 time
) external onlyOwner {
    require(threshold > 0);
    require(thresholdDivisor%10 == 0 && thresholdDivisor > 0);
    swapThreshold = (_tSupply * threshold) / thresholdDivisor;
    contractSwapTimer = time;
}

if (contractTokenBalance >= swapThreshold) {
    contractTokenBalance = swapThreshold;
    contractSwap(contractTokenBalance);
    lastSwap = block.timestamp;
}
```

Recommendation

The contract could ensure that it will not sell more than a reasonable amount of tokens in a single transaction. A suggested implementation could check that the maximum amount should be less than a fixed percentage of the exchange reserves. Hence, the contract will guarantee that it cannot accumulate a huge amount of tokens in order to sell them.

UFP - Unused Function Parameter

Criticality	Minor / Informative
Location	contracts/token.sol#L485
Status	Unresolved

Description

The function `_finalizeTransfer` has an unused function parameter `bool other`. This parameter is declared but not utilized anywhere within the function's body. Unused parameters can lead to confusion about the function's intended behavior and may suggest that there is incomplete implementation or redundant code.

```
function _finalizeTransfer(
    address from,
    address to,
    uint256 amount,
    bool takeFee,
    bool buy,
    bool sell,
    bool other
) internal returns (bool) {

    _tokenOwned[from] -= amount;
    uint256 amountReceived = (takeFee)
        ? takeTax(from, buy, sell, amount)
        : amount;
    _tokenOwned[to] += amountReceived;

    emit Transfer(from, to, amountReceived);
    return true;
}
```

Recommendation

It is recommended to review the purpose of the `bool other` parameter to determine if it was intended for use or if it is redundant. If the parameter is not needed, removing this parameter is advisable to enhance the code's clarity.

L02 - State Variables could be Declared Constant

Criticality	Minor / Informative
Location	contracts/token.sol#L16,92,93,94
Status	Unresolved

Description

State variables can be declared as constant using the constant keyword. This means that the value of the state variable cannot be changed after it has been set. Additionally, the constant variables decrease gas consumption of the corresponding transaction.

```
uint256 internal _tSupply = 100000000000000000000000000
string internal _name = "Oracle AI"
string internal _symbol = "ORACLE"
uint8 internal _decimals = 18
```

Recommendation

Constant state variables can be useful when the contract wants to ensure that the value of a state variable cannot be changed by any function in the contract. This can be useful for storing values that are important to the contract's behavior, such as the contract's address or the maximum number of times a certain function can be called. The team is advised to add the constant keyword to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	contracts/token.sol#L15,27,30,37,44,142
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.

```
uint256 constant taxDivisor = 10000

Fees public _taxRates =
        Fees({buyFee: 500, sellFee: 1000, transferFee: 0})

TaxPercentages public _taxPercentages =
        TaxPercentages({marketing: 70, dev: 30})
TaxWallets public _taxWallets
bool public _hasLiquidityBeenAdded = false
address _addr
```

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.

L07 - Missing Events Arithmetic

Criticality	Minor / Informative
Location	contracts/token.sol#L412
Status	Unresolved

Description

Events are a way to record and log information about changes or actions that occur within a contract. They are often used to notify external parties or clients about events that have occurred within the contract, such as the transfer of tokens or the completion of a task.

It's important to carefully design and implement the events in a contract, and to ensure that all required events are included. It's also a good idea to test the contract to ensure that all events are being properly triggered and logged.

```
_maxWalletSize = (_tSupply * percent) / divisor
```

Recommendation

By including all required events in the contract and thoroughly testing the contract's functionality, the contract ensures that it performs as intended and does not have any missing events that could cause issues with its arithmetic.

L08 - Tautology or Contradiction

Criticality	Minor / Informative
Location	contracts/token.sol#L312
Status	Unresolved

Description

A tautology is a logical statement that is always true, regardless of the values of its variables. A contradiction is a logical statement that is always false, regardless of the values of its variables.

Using tautologies or contradictions can lead to unintended behavior and can make the code harder to understand and maintain. It is generally considered good practice to avoid tautologies and contradictions in the code.

```
require(marketing>=0 && marketing<=100,'Percentage should be between 0 -
100')
```

Recommendation

The team is advised to carefully consider the logical conditions is using in the code and ensure that it is well-defined and make sense in the context of the smart contract.

L17 - Usage of Solidity Assembly

Criticality	Minor / Informative
Location	contracts/token.sol#L144
Status	Unresolved

Description

Using assembly can be useful for optimizing code, but it can also be error-prone. It's important to carefully test and debug assembly code to ensure that it is correct and does not contain any errors.

Some common types of errors that can occur when using assembly in Solidity include Syntax, Type, Out-of-bounds, Stack, and Revert.

```
assembly {
            size := extcodesize(_addr)
        }
```

Recommendation

It is recommended to use assembly sparingly and only when necessary, as it can be difficult to read and understand compared to Solidity code.

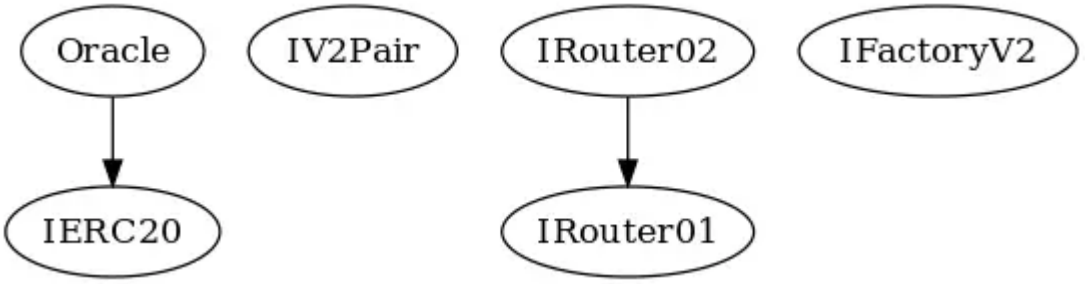
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Oracle	Implementation	IERC20		
		Public	Payable	-
	balanceOf	Public		-
	confirmLP	Public	✓	onlyOwner
	setPairAddress	Public	✓	onlyOwner
	isContract	Public		-
	preInitializeTransfer	Public	✓	onlyOwner
	transferOwner	External	✓	onlyOwner
	renounceOwnership	Public	✓	onlyOwner
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	allowance	External		-
	transfer	Public	✓	-
	approve	Public	✓	-
	approveContractContingency	Public	✓	onlyOwner
	transferFrom	External	✓	-

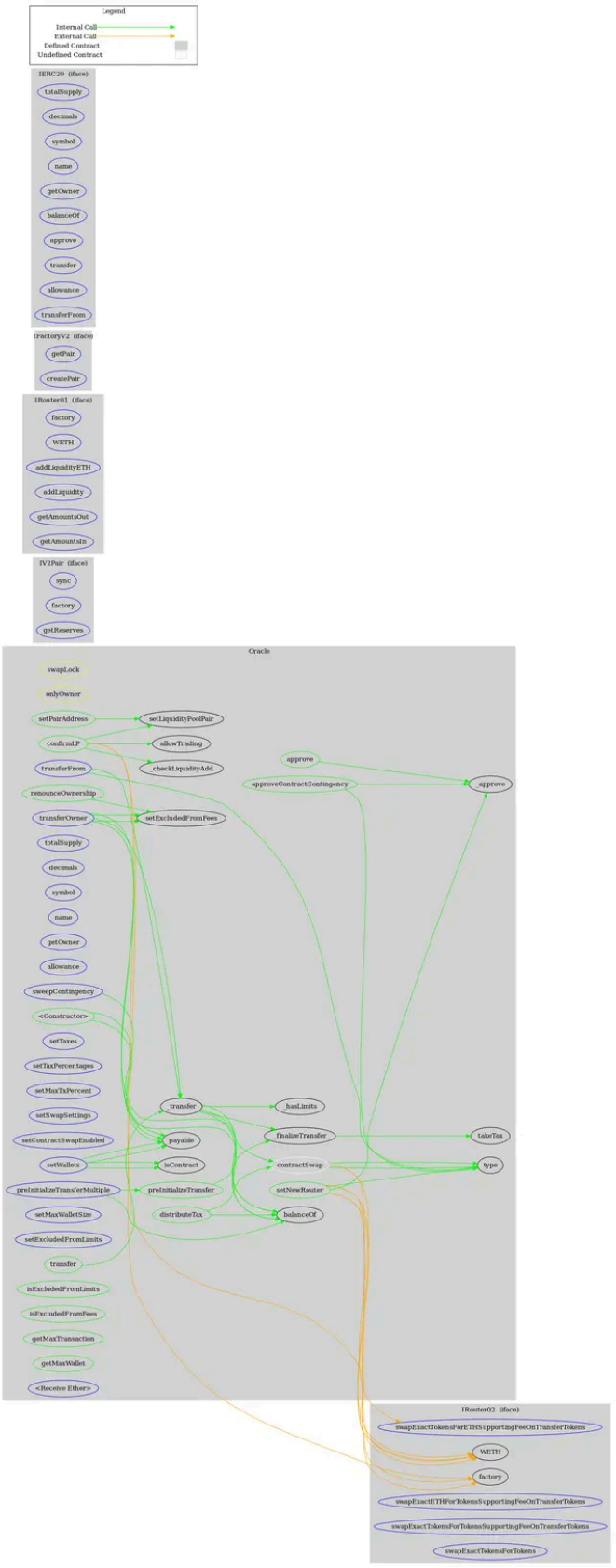
	setNewRouter	Public	✓	onlyOwner
	setLiquidityPoolPair	Public	✓	onlyOwner
	setTaxes	External	✓	onlyOwner
	setTaxPercentages	External	✓	onlyOwner
	setMaxTxPercent	External	✓	onlyOwner
	setSwapSettings	External	✓	onlyOwner
	setContractSwapEnabled	External	✓	onlyOwner
	setWallets	External	✓	onlyOwner
	preInitializeTransferMultiple	External	✓	onlyOwner
	allowTrading	Internal	✓	
	takeTax	Internal	✓	
	setMaxWalletSize	External	✓	onlyOwner
	setExcludedFromLimits	External	✓	onlyOwner
	sweepContingency	External	✓	onlyOwner
	contractSwap	Internal	✓	swapLock
	isExcludedFromLimits	Public		-
	isExcludedFromFees	Public		-
	setExcludedFromFees	Public	✓	onlyOwner
	getMaxTransaction	Public		-
	getMaxWallet	Public		-
	_finalizeTransfer	Internal	✓	
	_hasLimits	Internal		
	_transfer	Internal	✓	

	distributeTax	Public	✓	onlyOwner
	_approve	Internal	✓	
	_checkLiquidityAdd	Internal	✓	
		External	Payable	-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IERC20 (iface)
totalSupply
decimals
symbol
name
getOwner
balanceOf
approve
transfer
allowance
transferFrom
IFactoryV2 (iface)
getPair
createPair
IRouter01 (iface)
factory
WETH
addLiquidityETH
addLiquidity
getAmountsOut
getAmountsIn
IV2Pair (iface)
sync
factory
getReserves
Oracle
swapLock
onlyOwner
setPairAddress
setLiquidityPoolPair
confirmLP
allowTrading
transferFrom
checkLiquidityAdd
renounceOwnership
transferOwner
setExcludedFromFees
totalSupply
decimals
symbol
name
getOwner
allowance
sweepContingency
<Constructor>
setTaxes
setTaxPercentages
setMaxTxPercent
setSwapSettings
setContractSwapEnabled
setWallets
preInitializeTransferMultiple
setMaxWalletSize
setExcludedFromLimits
transfer
isExcludedFromLimits
isExcludedFromFees
getMaxTransaction
getMaxWallet
<Receive Ether>
approve
approveContractContingency
_approve
transfer
hasLimits
finalizeTransfer
takeTax
payable
isContract
contractSwap
type
preInitializeTransfer
setNewRouter
distributeTax
balanceOf
IRouter02 (iface)
swapExactTokensForETHSupportingFeeOnTransferTokens
WETH
factory
swapExactETHForTokensSupportingFeeOnTransferTokens
swapExactTokensForTokensSupportingFeeOnTransferTokens
swapExactTokensForTokens

Summary

Oracle AI contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. There are some functions that can be abused by the owner like stopping transactions. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats. 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